3/2013

# Datenschutz Nachrichten

36. Jahrgang
ISSN 0137-7767
9,00 Euro

Kommunaler Datenschutz

■ Die Gemeinsamen Datenschutzbeauftragten ■ Wann wird IT-Sicherheit kein Rechtsbruch mehr sein? ■ Live-Streaming ■ Prism, Tempora, Snowden… Analysen und Perspektiven ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

# Inhalt



# Termine

Samstag, 19. Oktober 2013
**DVD-Vorstandssitzung**
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 20. Oktober 2013
**DVD-Mitgliederversammlung**
Bonn.
dvd@datenschutzverein.de



Wir weisen darauf hin, dass wir am Vorabend, **19.10.2013** in einem Bonner Restaurant ab 19 Uhr ein Datenschutz-Gespräch mit Abendessen veranstalten. Zu diesem Gespräch hat der Bonner SPD-BT-Abgeordnete und stellvertretende Vorsitzende der BT-Fraktion der SPD Ulrich Kelber seine Teilnahme zugesagt. Er ist unter anderem als Vorreiter der Idee des „gläsernen Abgeordneten“ bekannt und setzt sich darüber hinaus nachdrücklich für Datenschutz ein. Mit Sicherheit wird er ein sehr kompetenter Gesprächspartner sein.
Wir würden uns freuen, wenn viele Mitglieder diese Gelegenheit ergreifen und uns beim Abendessen Gesellschaft leisten würden. Zur besseren Planung des Platzbedarfs bitten wir möglichst bis zum **12.10.2013** um Anmeldung in der Geschäftsstelle (E-Mail oder telefonisch). Der Veranstaltungsort in Bonn wird rechtzeitig bekanntgegeben.

Freitag, 1. November 2013
**Redaktionsschluss DANA 4/13**
Thema: Datenschutz-Grundverordnung und Europa

**DANA**
**Datenschutz Nachrichten**
ISSN 0137-7767
36. Jahrgang, Heft 3

**Herausgeber**
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

**Redaktion (ViSdP)**
Karsten Neumann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

**Layout und Satz**
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

**Druck**
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

**Bezugspreis**
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.



**Leserbriefe**
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

**Abbildungen, Fotos**
Frans Jozef Valenta,
Seite 128: David Valenta

# Editorial

Liebe Leserinnen, liebe Leser,

wenn Sie diese Seite aufschlagen, sind Sie vielleicht noch in bester Stimmung, die Sie von der Freiheit-statt-Angst-Demonstration in Berlin mit nach Hause gebracht haben. Und auch wir haben uns trotz des Ehrgeiz, Ihnen eine fachlich spezfisiche Ausgabe zur Kommunalverwaltung vorzulegen, keine Atempause von den populären, weltumspannenden Themen genehmigt und fiebern dem nächsten Einblick Edward Snowdens in die Realität unserer Kommunikation post 9/11 entgegen. Einiges davon finden Sie auch im Nachichtenteil. Zu Recht fragt Thilo Weichert in diesem Heft, ob uns das alles wirklich überraschen musste. In der Tat: Dass sich eine asymetrische Sicherheitspartnerschaft mit bestimmten Verbündeten nicht als Schonwaschgang für die Grundrechte in Deutschland erweisen würde, war abzusehen. Das Selbstbewusstsein dieser Verbündeten einerseits und wirre Reaktionen der höchsten politischen Entscheidungsträger in der Bundesrepublik andererseits werfen die Frage nach der Balance von Sicherheit durch den Staat und Sicherheit vor dem Staat wieder einmal neu auf. Apropos: Haben Sie Ihr Kreuz am 22. September an der richtigen Stelle gemacht?

Bitte werfen Sie noch einen kurzen Blick auf die Änderungen, die wir beim Preis der DANA vornehmen müssen (S. 113 in diesem Heft). Wir sehen uns auf der Mitgliederversammlung der DVD in Bonn am 20.10.2013. Bis dahin wünscht Ihnen wieder einmal starke Nerven beim Zeitunglesen und einen goldenen Herbst...

Sönke Hilbrans

## Autorinnen und Autoren dieser Ausgabe:

**Karsten Neumann**
Vorstandsmitglied der DVD, Landesbeauftragter für Datenschutz Mecklenburg-Vorpommern a.D., Associate Partner der 2B Advice GmbH,
neumann@datenschutzverein.de

**Ingo Ruhmann**
Wissenschaftlicher Referent und Gründungsmitglied des FIfF e.V..
Er beschäftigt sich u.a. mit Entwicklungen in der IT-Sicherheit und ist Lehrbeauftragter im Studiengang IT Security Management an der FH Brandenburg,
ruhmann@fh-brandenburg.de

**Anke Schröder**
Bereichsleiterin Datenschutz und IT-Sicherheit, Gemeinsame Datenschutzbeauftragte (udiszert) Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (ZV eGO M-V), Mitglied im Landesdatenschutzbeirat Mecklenburg-Vorpommern und Leiterin des Erfa-Kreises Mecklenburg-Vorpommern der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD),
anke.schroeder@evo-mv.de

**Dr. Thilo Weichert**
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel,
weichert@datenschutzzentrum.de

Anke Schröder

# Die Gemeinsamen Datenschutzbeauftragten

Ein Bericht über die Erfahrungen als externe behördliche Datenschutzbeauftragte in mecklenburg-vorpommerschen Gemeindeverwaltungen.

## Wie alles begann?

In 2006/2007 wurden in Mecklenburg-Vorpommern (M-V) das elektronische Rückmeldeverfahren und das Zentrale Informationsregister im Meldewesen eingeführt. Damit ist es möglich, elektronisch Meldedaten zwischen Behörden auszutauschen und Online-Melderegisterauskünfte zu erteilen. Bei der Einführung der Verfahren war der Landesdatenschutzbeauftragte M-V (LfDI M-V) umfassend beteiligt und hat den Gemeindeverwaltungen viele „Hausaufgaben" aufgegeben, damit die Verfahren sicher und datenschutzgerecht betrieben werden können. Es gab mehrhundertseitige Informationen zu rechtlichen Datenschutz- und IT-Sicherheitsanforderungen auf Grundlage des BSI IT-Grundschutzes.[1] Etwa zur gleichen Zeit gründeten, auf Initiative des Innenministeriums M-V und der kommunalen Spitzenverbände, 11 Städte und Ämter den Zweckverband „Elektronische Verwaltung in M-V" (ZV eGO M-V)[2], um die anstehenden Herausforderungen des eGovernment gemeinsam anzugehen. Mehrheitlicher Wunsch der Gründungsmitglieder war, dass der Zweckverband sich dem Thema Datenschutz widmet und die Verwaltungen bei der Erfüllung dieser Aufgaben unterstützt. Als erstes nahmen sie sich der „Datenschutzhausaufgaben" bei den elektronischen Meldeverfahren an und kamen auf die Idee, einen Vollzeitdatenschutzbeauftragten für mehrere Verwaltungen zu beschäftigten. Nach § 20 Absatz 1 Satz 2 Datenschutzgesetz M-V (DSG M-V[3]) „können mehrere Daten verarbeitende Stellen denselben behördlichen Datenschutzbeauftragten bestellen."[4] In Absprache mit dem LfDI M-V – der der Idee zwar skeptisch, aber wohlwollend gegenüberstand – wurde ein erster Gemeinsamer Datenschutzbeauftragter[5] angestellt, der zunächst 10 vorwiegend kleinere Gemeindeverwaltungen als externer behördlicher Datenschutzbeauftragter betreute. Das Modell[6] machte Schule, die anfängliche Skepsis des LfDI M-V schwand – und heute sind bereits drei Gemeinsame Datenschutzbeauftragte tätig.

## Gemeinsamer Datenschutzbeauftragter?

Natürlich denkt man sofort, ein Datenschutzbeauftragter vor Ort muss doch besser sein, als ein externer Berater. Das mag zwar theoretisch stimmen, hat aber mit der Praxis nichts zu tun. Zwar muss jede öffentliche Stelle in M-V einen behördlichen Datenschutzbeauftragten und sogar einen Vertreter schriftlich bestellen (vgl. § 20 Abs. 1, S. 1 DSG M-V)[7]; welche Möglichkeiten dieser zur Wahrnehmung seiner Aufgaben hat, steht aber auf einem anderen Blatt. Häufig existiert die Bestellung nur auf dem Papier, ein angemessenes Zeitkontingent zur Aufgabeerledigung ist aber nicht vorgesehen. Angesichts des oder oft der Hauptaufgabengebiete des „Betroffenen" ist eine Befassung mit dem Datenschutz in (kleineren) Gemeindeverwaltungen daher kaum zu leisten. Ein externer Vollzeitdatenschutzbeauftragter kann den Nicht-ständig-vor-Ort-zu-sein-Nachteil daher schon dadurch ausgleichen, dass er sich mit dem Datenschutz in fachlicher Hinsicht intensiv beschäftigen kann und weiß, an welchen Stellen Prüfungs- und Handlungsbedarf bestehen kann. Natürlich muss auch ein externer Beauftragter einen Überblick über die betreute Verwaltung und deren Beschäftigte haben – dieser lässt sich durch regelmäßige Vor-Ort-Besuche erlangen und stetig vertiefen. Auch durch Nutzung moderner Kommunikationsmittel lassen sich räumliche Entfernungen kurzfristig überbrücken. Damit bietet ein externer Datenschutzbeauftragter eine umfangreichere Sachkunde und durch die zusätzliche Nutzung von Synergieeffekten ein insgesamt besseres Kosten-Nutzen-Verhältnis. Als Externer unterliegt der Datenschutzbeauftragte i.d.R. auch keinem Interessenkonflikt und ist bei seinen Prüfungen, Beratungen und Empfehlungen objektiver, als es ein hausinterner Beauftragter sein kann. Die gesetzlichen Anforderungen an den Datenschutzbeauftragten – „keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben" ausgesetzt zu sein und „die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit" zu besitzen (vgl. § 20 Abs. 1 S. 3 DSG M-V)[8] – erfüllt ein externer daher oft besser, als ein interner Datenschutzbeauftragter. Mit der Bestellung eines Gemeinsamen Datenschutzbeauftragten haben daher viele Gemeindeverwaltungen einen Schritt zu mehr Datenschutz getan.

## Welche Themen?

Erste Kontaktperson des Gemeinsamen Datenschutzbeauftragten ist der aus dem Kreis der Beschäftigten der betreuten Verwaltung bestellte stellvertretende behördliche Datenschutzbeauftragten[9]. Dieser organisiert und koordiniert die Vor-Ort-Besuche, kennt die richtigen – nicht nur zuständigen, sondern auch zupackenden – Ansprechpartner für die verschiedenen Aufgaben und trägt mit zur Abarbeitung der Datenschutzaufgaben bei. Nach einer Bestandsaufnahme zum Stand von

Datenschutz und Datensicherheit in der Verwaltung gibt der Gemeinsame Datenschutzbeauftragte Empfehlungen zu notwendigen Maßnahmen und versucht, deren Umsetzung voranzutreiben – dafür braucht er häufig einen langen Atem.

(1) Zu einer der ersten Aufgaben des Gemeinsamen Datenschutzbeauftragten gehört es, Beschäftigtenschulungen zum Datenschutz durchzuführen und dabei die Beschäftigten (teilweise erstmalig) auf das Datengeheimnis zu verpflichten (vgl. § 6 DSG M-V).[10] Neben der Erläuterung des Rechts auf informationelle Selbstbestimmung, der gesetzlichen Grundlagen des Datenschutzrechts und praktischen Anleitungen zum datenschutzgerechten Verhalten am Arbeitsplatz gehören dazu auch Hinweise zum Beschäftigtendatenschutz. Die Schulungen werden folgend in regelmäßigem Abstand (2-3 Jahresrhythmus) durchgeführt. Dies verfestigt das Thema an sich und bietet die Möglichkeit, neue Themen gemeinsam zu diskutieren. Gleichzeitig verdeutlicht die Behördenleitung durch „Gestattung“ der Schulung die Wichtigkeit des Themas, denn Schulungsmaßnahmen werden bei weitem nicht zu jedem erforderlichen Themenbereich regelmäßig durchgeführt. Die Sensibilisierung der Beschäftigten für den Datenschutz wird darüber hinaus – oder besser insbesondere – durch viele persönliche Gespräche im Rahmen der regelmäßigen Vor-Ort-Besuche des Gemeinsamen Datenschutzbeauftragten in den Verwaltungen bewirkt. Durch die Cartoon-Ausstellung „Datenschutz – Nie war er so wertvoll wie heute!“[11] mit Werken von Reinhard Alff, die durch die Verwaltungsgebäude „wandert“, werden die Beschäftigten, wie auch die Verwaltungsbesucher in humorvoller Weise auf den Datenschutz aufmerksam gemacht.

(2) Ein Thema, welches die betreuten Verwaltungen meist besonders interessiert, ist das Verfahrensverzeichnis mit den Verfahrensbeschreibungen für jedes von ihnen eingesetzte (automatisierte) Verfahren. In den Beschreibungen sind die Zwecke, Rechtsgrundlagen und die Art und Weise der Datenverarbeitung, der Kreis der Betroffenen, Datenübermittlungen und umgesetzte Sicherheitsmaßnahmen zu beschreiben (vgl. § 18 DSG M-V).[12] Sie dienen als Grundlage für die ggf. notwendige Vorabkontrolle durch den behördlichen Datenschutzbeauftragten und die Freigabe der Verfahren durch den Leiter der datenverarbeitenden Stelle (§ 19 DSG M-V). Die Beschreibungen sind von der datenverarbeitenden Stelle anzufertigen und dem Datenschutzbeauftragten zu übermitteln – so zumindest die Theorie. In der Praxis denken die Verwaltungen aber häufig, die Anfertigung dieser Dokumentationen sei (Haupt)Aufgabe des behördlichen Datenschutzbeauftragten – hier ist zunächst entsprechende Aufklärungsarbeit zu leisten. Letztlich unterstützt der Gemeinsame Datenschutzbeauftragte die Verwaltungen aber auch insoweit. So werden Mustervorlagen zur Ausfüllung zunächst durch die Fachverfahrensanbieter und dann durch die zuständigen Beschäftigten erstellt. Durch persönliche Gespräche in den jeweiligen Fachbereichen zu den tatsächlichen Verfahrensabläufen und Hintergründen der Fachaufgabe erhält der Gemeinsame Datenschutzbeauftragte nähere Informationen und kann dann weitere konkretere Hinweise zur Erstellung der Verfahrensbeschreibungen liefern. Ein wichtiger Punkt ist in diesem Zusammenhang auch die Umsetzung notwendiger Sicherheitsmaßnahmen. Ergibt sich im Gespräch, dass z.B. regelmäßig Daten per E-Mail an eine andere Behörde übermittelt werden, kann gezielt über die Notwendigkeit von Verschlüsselung aufgeklärt und zur Etablierung entsprechender Verfahren beigetragen werden.

(3) Datenschutz funktioniert nur, wenn die erforderlichen Daten- und IT-Sicherheitsmaßnahmen ergriffen werden. Der LfDI M-V verweist insoweit stetig auf den BSI IT-Grundschutz.[13] Dieser bietet eine Vielzahl konkreter Maßnahmenempfehlungen, im BSI-Standard 100-2[14] Hinweise für die Vorgehensweise bei der Umsetzung der Empfehlungen und mit dem GSTOOL[15], ein (u.a. für unmittelbare Kommunalverwaltungen kostenfreies) Anwendungswerkzeug zur Erstellung von Sicherheitskonzepten. Nicht nur kleine Gemeindeverwaltungen sind mit dem BSI-IT-Grundschutz häufig überfordert. Zwar erkennen die Behördenleitungen immer häufiger ihre diesbezügliche Verantwortung, sehen sich angesichts ihrer fachlich personellen Möglichkeiten aber kaum in der Lage, in strukturierter und umfassender Weise die notwendigen Konzeptionen und insbesondere Dokumentationen zu bewerkstelligen. Das heißt aber nicht, dass es keine Daten- und IT-Sicherheit in den Verwaltungen gibt. Die grundlegenden Sicherheitsanforderungen sind i.d.R. insbesondere durch entsprechende Maßnahmen externer EDV-Dienstleister erfüllt, z.B. die Abschottung des Behördennetzwerkes durch Firewalls, den Einsatz zentraler und dezentraler Virenschutzsysteme, den Passwortschutz für IT-Systeme, abgeschottete Serverräume usw. Eine Dokumentation dieser Maßnahmen gibt es aber kaum. Die Dokumentation von IT-Sicherheitskonzepten nach IT-Grundschutz ist nicht Aufgabe des behördlichen Datenschutzbeauftragten (auch wenn dies häufig angenommen wird), dieser hat vielmehr darauf hinzuwirken, dass solche Konzeptionen und Dokumentationen erarbeitet werden. Die Gemeinsamen Datenschutzbeauftragten geben insoweit konkrete Empfehlungen zu umzusetzenden Maßnahmen z.B. zur notwendigen Laufwerks- und Schnittstellensperre, Verbesserung der Passwortkonventionen auch in den einzelnen Fachverfahren, Optimierung der Rechtestrukturierung, Notwendigkeit von Verschlüsselungsverfahren, Klimatisierung des Serverraums usw. Für die häufig fehlenden Organisationsregeln entwerfen sie konkrete Regelungsvorschläge, z.B. für Dienstanweisungen zur Nutzung von IT-Systemen, mobilen Speichermedien, Smartphones oder Dienstvereinbarungen zur Nutzung der Kommunikationssysteme Internet, E-Mail und Telefon. Bis zur Inkraftsetzung dieser ist es oft ein langer Weg mit viel Überzeugungsarbeit; sowohl auf Seiten der Behördenleitung, als auch auf Seiten des Personalrates.

E-Governmentverfahren (z.B. elektronische Personenstandsregisterführung, elektronisches Fundsachenregister) werden meist als zentrale Verfahren in Rechenzentren betrieben, die von den Gemeindeverwaltungen genutzt werden können oder müssen. Auch das allgemeine Hosting von Fachverfahren (z.B. Sitzungsdienstprogramme) in

Rechenzentren nimmt zu. Dies führt zu einer Professionalisierung der Daten- und IT-Sicherheit. Werden diese Verfahren als Gemeinsame Verfahren i.S.v. § 3 Absatz 10 i.V.m Absatz 5 DSG M-V[16] ausgestaltet, führt dies dazu, dass die Datenschutz-Verantwortung auf mehrere Schultern verteilt wird (anders bei der Auftragsdatenverarbeitung, bei der der Auftraggeber immer in der Gesamtverantwortung ist). Dieses Modell der Verantwortungsteilung muss angesichts der zunehmenden Komplexität und insbesondere bei Ebenen-übergreifenden E-Government-verfahren noch weiter ausgebaut werden. Die Verantwortungsübernahme darf dabei nicht nur bei den Gemeinden verbleiben, sondern muss auch die Landes- und Bundesebene einbeziehen. Die Verfahren zur Ausgestaltung und Wahrnehmung dieser gemeinsamen Verantwortung müssen noch entwickelt werden. Denkbar wären beispielsweise zentrale Prüfverfahren[17], Aufgaben des übertragenen Wirkungskreises der Gemeinden betreffend, die vom jeweiligen „Aufgabensteller“ (Bund oder Land) auf eigene Kosten (als Teil der Verantwortungsübernahme) wahrgenommen und schon bei der Aufgabeübertragung mit vorgesehen werden. Es könnte also z.B. ein „Bundesprüfer“ ins Rechenzentrum kommen, das konkret umgesetzte Personenstandsregisterverfahren hinsichtlich Datenschutz- und Datensicherheitskonformität prüfen und anschließend im Ergebnis die Ordnungsmäßigkeit feststellen. Dieses Ergebnis würde dann gleichzeitig für die Gemeinden bedeuten, dass sie ihre datenschutzrechtlichen Verpflichtungen erfüllt haben und grundsätzlich von weiteren Prüfpflichten entbunden sind. Regelmäßige Wiederholungsprüfungen sind angesichts der rechtlichen und technischen Weiterentwicklungen natürlich notwendig.

(4) Auch Auftragsdatenverarbeitungen (ADV) sind in den Gemeindeverwaltungen ein Thema. Werden personenbezogene Daten im Auftrag der Verwaltungen durch Dritte verarbeitet, müssen die Dritten auch unter Datenschutzgesichtspunkten ausgewählt und mit ihnen ausreichende Datenschutzregelungen schriftlich vereinbart werden (vgl. § 4 DSG§ M-V).[18] Insbesondere bei Wartungs-, Fernwartungs- und anderen Hilfstätigkeiten fehlen solche Regelungen häufig. Hier gilt es, konkrete Vorschläge zu unterbreiten und teilweise auch den Vertragspartnern „schmackhaft“ zu machen. Manchmal funktioniert dies auch sehr leicht: man bekommt den unterschriebenen ADV-Vertrag schnell zurück und kurze Zeit später kommt die Frage: „Sie wollen doch nicht wirklich bei uns prüfen kommen?“

(5) Mittlerweile ist auch jede Gemeindeverwaltung im Internet präsent – es gilt somit auch dabei entsprechende Datenschutzregeln einzuhalten. Die Umsetzung der notwendigen Datenschutzerklärungen[19] und die Beratung über erforderliche Einwilligungen für bestimmte Veröffentlichungen, insbesondere von Fotos[20], spielen in der Beratungspraxis eine große Rolle. Immer häufiger werden beispielsweise persönliche Kontaktdaten der kommunalen Gremienmitglieder und vielfältige Informationen aus dem Gemeindeleben mit Fotos auf den Homepages veröffentlicht. Beim Einsatz von Bürgerinformationssystemen werden auch Niederschriften von öffentlichen kommunalen Gremiensitzungen und öffentliche Beschlussvorlagen im Internet veröffentlicht. Zwar waren diese Informationen auch vorher schon öffentlich zugänglich – bei einem Besuch im Rathaus kann jeder öffentliche Niederschriften einsehen. Die Onlineveröffentlichung stellt aber eine ganz andere Qualität und Quantität dar, der durch eine datenschutzgerechte Gestaltung der Informationen ausreichend Rechnung getragen werden muss. Auch die Themen Teilnahme an Sozialen Netzwerken und Nutzung von „Gefällt-mir-Buttons“ spielt eine zunehmende Rolle. Wenn entgegen der Empfehlung des Gemeinsamen Datenschutzbeauftragten diese dennoch genutzt werden, muss zumindest auf die Intensivierung der diesbezüglichen Informationspflichten gedrängt werden (z.B. Impressumpflicht, Zusatzinformationen in der Datenschutzerklärung, 2-Klick-Lösung).

(6) Im Laufe der Zusammenarbeit werden neben grundlegenden Datenschutzfragen auch Spezialthemen aus einzelnen Fachbereichen aufgegriffen, z.B. zur datenschutzgerechten Konfiguration der behördeninternen Melderegisterkurzauskunft oder zum Datenschutz im Zusammenhang mit Wahlen. Diesbezüglich notwendige Datenschutzmaßnahmen lassen sich oft leichter umsetzen, als die grundlegenden Gesamtanforderungen, da sie insgesamt überschaubarer und bezogen auf einen konkreten Anwendungsfall leichter integrierbar sind. Insbesondere aus kleineren Gemeindeverwaltungen erhalten die Gemeinsamen Datenschutzbeauftragten auch immer wieder ganz spezielle Anfragen, wie z.B. „Darf einem vom Amtsgericht bestellten Sachverständigen zur Verkehrswertermittlung eines Privatgrundstücks auf Anfrage mitgeteilt werden, ob und ggf. in welcher Höhe öffentliche Lasten auf dem Grundstück liegen?“ Teilweise betreffen die Anfragen auch Standardkenntnisse des jeweiligen Fachbereichs, wie z.B. „Darf ich auf Anfrage Auskunft zu Name, betrieblicher Anschrift und angezeigter Tätigkeit eines Gewerbetreibenden geben?“ Durch die geringer werdende Personaldecke und die damit verbundene Kumulation mehrerer Fachaufgaben bei einzelnen Beschäftigten ist es diesen nicht mehr möglich, hinsichtlich ihrer gesamten Aufgabenbereiche auf dem jeweils aktuellen Fachstand zu sein. Bedenkt man, dass Gemeindeverwaltungen ca. 300 – 500 Gesetze umzusetzen haben, ist leicht nachvollziehbar, dass ein Beschäftigter einer 20-Mann-Verwaltung bei durchschnittlich von ihm zu berücksichtigenden 100 Gesetzen nicht immer auf dem neuesten Stand sein kann. Hier ist auch die Fachaufsicht gefordert, im Rahmen von Erlassen, Informationsschreiben und Fachbesprechungen konkrete Hinweise zu gesetzlichen Datenübermittlungsbefugnissen und weiteren Datenschutzregelungen zu geben.

Insgesamt hat sich das Modell Gemeinsamer Datenschutzbeauftragter gut etabliert und bewährt. In den betreuten Verwaltungen konnte das Datenschutzniveau signifikant verbessert werden. Ein Ende dieser Arbeit ist aber sicherlich nicht in Sicht.

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

2 http://www.ego-mv.de

3 http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&doc.id=jlr-

DSGMVpG2&doc.part=X&doc. origin=bs&st=lr

4 Ähnliche Formulierungen gibt es auch in anderen Bundesländern (vgl. z.B. § 32a Abs. 1 S. 3 DSG NRW, § 11 Abs. 1 S. 3 SächsDSG). Nach § 4f Abs. 2 S. 3 Bundesdatenschutzgesetz (BDSG) kann „zum Beauftragten für den Datenschutz (kann) auch eine Person außerhalb der verantwortlichen Stelle bestellt werden".

5 http://www.ego-mv.de/index.php?id=36

6 Vergleichbare Modelle gibt es auch in anderen Bundesländern, z.B. schon langjährig beim Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO) (https://www.kdo.de/datenschutzbeauftragter.php).

7 Nicht in jedem Bundesland gibt es eine Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten. In Schleswig-Holstein und Sachsen beispielsweise ist die Bestellung fakultativ (vgl. § 10 Abs. 1 LDSG SH bzw. § 11 Abs. 1 SächsDSG).

8 Weitgehend gleichlautende Anforderungen stellen auch das BDSG (§ 4f Abs. 2) und die Landesdatenschutzgesetze (vgl. z.B. § 7a Abs. 1 S. 2 BbgDSG, §32a Abs. 1, S. 2 und Abs. 2 S.3 DSG NRW).

9 Im Gegensatz zum BDSG sieht das DSG M-V verpflichtend die Bestellung eines stellvertretenden Datenschutzbeauftragten vor, § 20 Absatz 1 DSG M-V.

10 Eine entsprechende Verpflichtung kennen auch das BDSG (§ 5) und einige Landesdatenschutzgesetze (vgl. z.B. § 6 SächsDSG).

11 Die Ausstellung kann gegen eine Bearbeitungsgebühr beim ZV eGO M-V ausgeliehen werden: http://www.ego-mv.de/index.php?id=132

12 Verfahrensverzeichnisse und -beschreibungen sehen auch das BDSG (§ 4d, § 4e) und die Landesdatenschutzgesetze (vgl. z.B. § 8 BbgDSG, § 7 LDSG SH i.V.m. der Datenschutzverordnung SH) vor.

13 vgl. Fußnote 1

14 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile

15 https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.html

16 Eingeführt mit Artikel 2 „Viertes Gesetz zur Deregulierung und zum Bürokratieabbau vom 28.10.2010" (vgl. GVOBl. M-V 2010 S. 615 ff.): „Gemeinsame Verfahren sind automatisierte Verfahren, die aus mindestens zwei eigenständigen automatisierten Teilverfahren bestehen, für die verschiedene Daten verarbeitende Stellen verantwortlich sind." Seit Januar 2012 gibt es (ähnliche) Gemeinsame Verfahren auch in Schleswig-Holstein (§ 8 LDSG SH).

17 Solch ein „Prüfverfahren auf Bundesebene" wird momentan auf Ebene der Innenministerien der Länder (auf Anregung Baden – Württembergs) bzgl. des Personenstandregisterverfahrens diskutiert; allerdings nur in Bezug auf die eingesetzten Programme an sich (mit Bezug auf die in § 12 der Verordnung zur Ausführung des Personenstandgesetzes vorgesehene Herstellererklärung).

18 Regelungen zur Auftragsdatenverarbeitung finden sich auch im BDSG (§ 11) und in den Landesdatenschutzgesetzen (vgl. z.B. § 7 SächsDSG, § 11 DSG NRW).

19 vgl. § 13 Abs. 1 Telemediengesetz

20 vgl. § 22 (Einwilligungserfordernis) und § 23 (Ausnahmen) Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie

Ingo Ruhmann

# Wann wird IT-Sicherheit kein Rechtsbruch mehr sein?

**Das Bundesverfassungsgericht hat nach dem Grundrecht auf informationelle Selbstbestimmung das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" definiert. Die IT-Sicherheit ist das Arbeitsfeld, in dem der Schutz dieser beiden fundamentalen Grundrechte der Informationsgesellschaft umgesetzt werden muss. Die Praxis steht zu den Anforderungen des Rechts jedoch in einem deutlichen Kontrast. Die IT-Sicherheit von Webangeboten beruht in der Regel auf der Auswertung von Daten über Nutzerzugriffe. Für eine Speicherung und Auswertung solcher Daten fehlt jede Rechtsgrundlage. Das vom Bundesinnenministerium vorgelegte „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" könnte hier den IT-Sicherheitsverantwortlichen rechtliche und praktische Hilfen geben. Besserung ist jedoch nicht in Sicht.**

Vielleicht erinnert sich noch jemand daran, aus welchen Gründen die damalige Bundesjustizministerin Brigitte Zypries 2007 vom Landgericht Berlin unter Androhung eines Zwangsgeldes in Höhe von 250.000 Euro rechtskräftig dazu verurteilt wurde, im Webauftritt des Justizministeriums jede Protokollierung von IP-Nummern über das Ende des jeweiligen Nutzungsvorgangs hinaus abzustellen.[1]

Das Urteil war Endpunkt eines Rechtsstreits[2] gegen die Protokollierung von Nutzerdaten durch Betreiber von Webseiten – rechtlich: Telemedienanbieter. Die Klage richtete sich konkret gegen die Ungesetzlichkeit der Nutzerdatenprotokollierung, wie sie durch Bundesministerien, vor allem aber das Bundeskriminalamt (BKA), praktiziert wurde. Das BKA hatte im Zuge von Ermittlungen gegen eine

„militante Gruppe" sein Webangebot als klassischen Honeypot genutzt. Die Nutzerzugriffe auf die Webseiten mit Informationen über die entsprechenden Fahndungsmaßnahmen wurden gezielt protokolliert, um die Nutzer zu ermitteln.[3]

Urteil und Zwangsgeld gegen eine Ministerin führten bei Bundesregierung und Parlament schnell zu weiteren Aktivitäten. So erklärte die Bundesregierung 2007 auf Anfrage der Fraktion der Linken zur Notwendigkeit der Protokollierung von IP-Nutzerdaten für Zwecke der IT-Sicherheit:

*„Die Speicherung ist insbesondere aus Sicherheitsgründen notwendig: Die Bundesverwaltung ist kontinuierlich massiven und hoch professionellen Angriffen aus dem Internet ausgesetzt und der durch die Angriffe verursachte Kommunikationsverkehr übertrifft seit langem den regulären Kommunikationsverkehr. Zur Abwehr dieser Angriffe und zur Aufrechterhaltung des Behördenbetriebs sind zahlreiche Sicherheitsmaßnahmen notwendig. Dazu gehört zwingend die Speicherung der IP-Adressen, um Angriffsmuster erkennen und Gegenmaßnahmen (z. B. das Sperren bestimmter, für den Angriff genutzter IP-Adressen) einleiten zu können. Ohne diese Daten ist eine Abwendung der kontinuierlichen Angriffe nicht möglich."*[4]

Trotz der „zwingenden Notwendigkeit" zur Speicherung von IP-Daten für IT-Sicherheitszwecke bewertete die Bundesregierung die Rechtmäßigkeit der Speicherung von IP-Nummern jedoch deutlich vorsichtiger:

*„Inwieweit IP-Adressen personenbezogene Daten darstellen, ist nicht abschließend geklärt. Mit dem in der Kleinen Anfrage in Bezug genommenen Urteil des AG Berlin liegt nach hiesiger Kenntnis erstmals eine Gerichtsentscheidung vor, nach der IP-Adressen nicht nur für den Zugangsanbieter, der diese Adressen vergibt, sondern auch für den Anbieter eines (Medien-) Dienstes personenbezogene Daten sind, obwohl der Diensteanbieter einen Personenbezug allenfalls mit Hilfe des Zugangsanbieters herstellen könnte."*[5]

Der entscheidende Punkt war und ist genau die Frage, wie Telemedienanbieter mit IP-Nummern umgehen und in welchem Umfang sie IP-Nummern natürlich auch zur Erkennung von Manipulationsversuchen speichern und auswerten dürfen.

Die damals ungeklärte Frage, ob IP-Nummern personenbezogene Daten seien und vom Grundrecht auf informationelle Selbstbestimmung geschützt sind, ist mittlerweile höchstrichterlich geklärt: Das Bundesverfassungsgericht (BVerfG) urteilte im Januar 2012 über Sammlung und Abruf von IP-Adressen.[6]

*„Insbesondere fallen unter den Schutz der informationellen Selbstbestimmung auch personenbezogene Informationen zu den Modalitäten der Bereitstellung von Telekommunikationsdiensten."*[7]

Zu diesen gehörten auch dem Gericht zufolge Kennungen wie etwa IP-Nummern. Zwar unterließ das Verfassungsgericht die eindeutige Gleichsetzung jedweder IP-Nummer mit personenbezogenen Daten, begründete dies aber mit der Differenzierung, dass derzeit statische IP-Adressen vornehmlich für Geschäftskunden bedeutsam seien. Anders werde dies erst durch die absehbare Entwicklung hin zu dauerhaft statisch vergebenen IP-Adressen im IPv6.[8] Über die für Privatkunden typische Vergabe dynamischer IP-Adressen urteilte das Gericht jedoch:

*„Die Identifizierung von dynamischen IP-Adressen ermöglicht in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet. Zwar hat sie eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie jedoch eine erheblich größere Persönlichkeitsrelevanz und kann mit ihr nicht gleichgesetzt werden".*[9]

Die höchstrichterliche Diskussion der Funktion von IP-Nummern im Datenverkehr lässt daher keinen Zweifel mehr daran, dass IP-Nummern personenbezogene Daten sind. Die rechtliche Konsequenz daraus ist aber, dass solche personenbezogenen Daten nur auf gesetzlicher Grundlage oder nach Einwilligung der Nutzer gespeichert werden dürfen. Und zwar durch Telemedienanbieter ebenso wie durch jeden Telekommunikationsprovider – egal ob zu Werbezwecken oder für die IT-Sicherheit. Oder anders: Die Protokollierung von vollständigen IP-Nummern zu Zwecken der IT-Sicherheit ist ein Verstoß gegen Persönlichkeitsrechte, der nur auf Grundlage einer gesetzlichen Ermächtigung oder Einwilligung zulässig ist.

Eine Rechtsgrundlage für die Protokollierung von personenbezogenen Daten zu Sicherheitszwecken gibt es für Telekommunikationsprovider. Das Telekommunikationsgesetz (TKG) erlaubt es in §100 den Betreibern „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer [zu] erheben und [zu] verwenden".

Darauf können sich IT-Sicherheitsverantwortliche bei der Protokollierung von IP-Nummern aber nicht berufen. Für die klassischen Webangebote wie Webseiten zur Information, aber genauso auch Webshops, Cloud-Speicher oder komplexe webbasierte Softwaredienste gilt das Telemediengesetz (TMG). Ein Ziel des TMG war die anonyme oder pseudonyme Nutzung des Internets. Daher dürfen Anbieter keine oder nur möglichst wenige Daten erheben, zumal im Internet zwischen Anbietern und Nutzern von Telemedien vielfach kein Vertragsverhältnis besteht, das die Rechtslage zwischen beiden Seiten individuell regeln könnte. Daher verbietet das TMG in §12 ausdrücklich die beliebige Speicherung personenbezogener Daten in Webangeboten. Zulässig ist allein die zur Kommunikation nötige Speicherung und Verarbeitung der Daten, die am Ende der Nutzung umgehend zu löschen sind:

**TMG §13 (4) Nr. 2**

*Der Diensteanbieter hat [..] sicherzustellen, dass [..] die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht [..] werden.*

Und um die Frage von Nutzungsdaten – wie etwa die IP-Nummern der zugreifenden Benutzer – zweifelsfrei zu definieren, erlaubt §15 TMG ein „erheben und Verwenden" personenbezogener Nutzerdaten – als da sind:

*„1. Merkmale zur Identifikation des Nutzers,*
*2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und*
*3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien“*
nur für Abrechnungszwecke, wenn eine Vertragsbeziehung besteht, nicht aber bei anonym nutzbaren Angeboten. Allein „bei Verwendung von Pseudonymen“ ist es zulässig, Nutzungsprofile für „Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung“ der Telemedien zu erstellen.

Dieser Rechtsrahmen

- erlaubt, IP-Nummern von Nutzern eines Webangebotes zu verarbeiten, solange die aktuelle Nutzung andauert,
- erfordert die Löschung der Daten und IP-Nummern unmittelbar nach Ende dieser Nutzung
- oder lässt die Bildung und Sammlung pseudonymisierter Nutzungsprofile zu, wie sie etwa durch wirksame Verkürzung oder Veränderung der IP-Nummer möglich sind.

Unzulässig ist jedoch, vollständige IP-Nummern zu Zwecken der IT-Sicherheit dauerhaft zu speichern. Und um die Ernsthaftigkeit dieser Vorschrift besonders herauszuheben, sieht das TMG für Zuwiderhandlungen einen der sehr wenigen Bußgeldtatbestände vor.

Damit haben IT-Sicherheitsverantwortliche im alltäglichen Fall eines Angriffs auf ein Webangebot keine legal gesammelten Daten in der Hand, die für eine juristische Lösung nutzbar wären. Selbst bei der Speicherung von pseudonymisierten Daten muss man als Praktiker wohl besser ausblenden, dass IT-Sicherheit als gesetzlich legitimierter Zweck einer Datenspeicherung im Telemedienrecht schlicht nicht vorgesehen ist. Für die Klärung der überwiegenden Zahl Internet-basierter IT-Sicherheitsvorfälle auf juristischem Weg gibt es damit in Deutschland keine rechtliche Grundlage.

Deshalb war spätestens nach dem Urteil des Bundesverfassungsgerichts 2012 die Frage zwangsläufig, wie IT-Sicherheitsverantwortliche eine rechtskonforme Detektion von IT-Sicherheitsvorfällen ohne eine Rechtsgrundlage für die Speicherung von IP-Nummern bei Verdachtsfällen oder einem Angriff realisieren sollten.

## Vertane Chancen zu einer Lösung

Nun wäre es mit Sicherheit eine absurde Vermutung, dass Betreiber von Botnetzen oder andere Verbreiter von Malware erst vor Gericht ziehen, dort bei ihrem ausgesuchten Opfer die Abschaltung einer IP-Protokollierung erwirken, um dann unbeobachtet ihr Schadwerk zu vollbringen.

Anders herum wird das Problem akut: Wie kann ein IT-Sicherheitsverantwortlicher vor Gericht Protokolldaten als Beweis für eine Manipulation verwenden, wenn diese Daten von einem fähigen Strafverteidiger als unrechtmäßig gesammelte Beweismittel unbrauchbar gemacht werden?

Warum sollte sich ein durch IT-Sicherheitsvorfälle Geschädigter dann überhaupt einer juristischen Klärung seines Problems aussetzen? Der Ausgang eines Rechtsstreits wird zum ungewissen Risiko, zumal Richter bei Technikthemen die Gesetze ebenso wie höchstrichterliche Urteile keineswegs vorhersagbar interpretieren. Ein geschädigter Kläger, der vor Gericht zieht, könnte daher als Beklagter enden.

Eine erste Möglichkeit zu einer Lösung des Problems bot sich mit der 2009 in Kraft getretenen Novelle des BSI-Gesetzes, mit dem die Bundesregierung auf ihre Weise auf das Berliner Urteil gegen Justizressort und Ministerin Zypries reagierte. Statt einer Lösung für die Allgemeinheit wurde eine juristische Speziallösung gewählt.

So wurde in § 5 des BSI-Gesetzes einzig und allein das Bundesamt für die Sicherheit in der Informationstechnik (BSI) dazu ermächtigt – so der Wortlaut des Gesetzes – „Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, [zu] erheben und automatisiert aus[zu]werten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist“.

Damit ist ausschließlich das BSI für die Webangebote der Bundesverwaltung in der komfortablen Lage, alle nötigen Daten rechtsfest erheben und auswerten zu können. Weder das BKA noch der Bundesnachrichtendienst oder irgendeine andere Bundes- oder Landesbehörde oder ein Unternehmen sind rechtlich dazu berechtigt, die üblichen IP-Protokolldateien für IT-Sicherheitszwecke zu sammeln und auszuwerten. Dies gilt ebenso für CERTs, IT-Sicherheitsunternehmen und andere IT-Sicherheitsprofis, deren tägliche Arbeit die Analyse von Datenverkehren bei Telemedien ist: Sie alle operieren bei der Auswertung von IP-Daten eindeutig im rechtswidrigen Raum.

Unternehmen können weiterhin das rechtliche Risiko eingehen, denn die Wahrscheinlichkeit einer Klage dürfte für sie gering sein. In Behörden sieht das dagegen anders aus. Eingedenk des Urteils gegen das Bundesjustizressort und Frau Zypries ist die Rechtslage eindeutig. Eine gleichartige Klage gegen andere Behörden wäre sehr erfolgversprechend und obendrein kostenfrei. Auch eine Datenschutzbehörde könnte die rechtskonforme Datenspeicherung zu IT-Sicherheitszwecken einfordern und eine Rüge aussprechen. Behördliche IT-Sicherheitsverantwortliche, die heute gleichwohl die nicht-pseudonymisierte IP-Protokollierung weiter laufen lassen und damit vorsätzlichen Rechtsbruch begehen, müssen daher im Klagefall mit personalrechtlichen Konsequenzen und der Abwälzung der entstehenden Kosten durch ihren Dienstherren rechnen. Eine ungemütliche Lage, in der niemand gern stecken mag.

## Das geplante IT-Sicherheitsgesetz

Diese Ausgangslage böte daher genug Anlass, der IT-Sicherheit für Webangebote in Deutschland endlich eine legale Grundlage zu geben. Passend dafür wäre, dies im Zuge des im Frühjahr 2013 zur Diskussion gestellten „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“[10] umzusetzen.

Zweck des geplanten Gesetzes ist es, die Betreiber kritischer IT-Infrastrukturen „in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesund-

heit, Wasser, Ernährung sowie Finanz- und Versicherungswesen“ – dem Anfang März verschickten Gesetzesentwurf zufolge – dazu zu verpflichten, „Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind“ und dem „Stand der Technik“ entsprechen. Sicherheitsaudits sollen die Wirkung der Maßnahmen validieren. Telekommunikationsunternehmen werden in ähnlicher Weise zu höheren Sicherheitsstandards verpflichtet.

Damit wird der als Schutzniveau für IT-Technologie in § 9 des Bundesdatenschutzgesetzes seit Jahren vorgeschriebene „Stand der Technik“, der bisher für alle Betreiber verpflichtend war, die personenbezogene Daten „erheben, verarbeiten oder nutzen“, nahezu wortgleich auf den Betrieb von Anlagen und Systemen ausgeweitet.

IT-Sicherheitsvorfälle sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umgehend gemeldet werden, das daraus ein Lagebild zusammenstellt. Die Verfolgung von Computerkriminalität, die gegen „sicherheitsempfindliche Behörden oder Einrichtungen des Bundes“ gerichtet ist, soll nach Artikel 2 des Gesetzentwurfs dem Bundeskriminalamt (BKA) übertragen werden.

Abgesehen von der gut 15-jährigen Historie des Schutzes kritischer Infrastrukturen, der nie über eine freiwillige Mitwirkung der Industrie hinausgekommen ist, trat die Bundesregierung mit der Idee an, durch gesetzliche Vorschriften den Schutz kritischer Infrastrukturen gegen Manipulationen an IT-Systemen zu verbessern. Doch verpflichtet der Gesetzesvorstoß zum IT-Sicherheitsgesetz die IT-Sicherheitsverantwortlichen dazu, IT-Sicherheitsvorfälle zu melden, die höchst wahrscheinlich aufgrund einer Sammlung und Auswertung von Protokolldaten widerrechtlich erhoben, ausgewertet und ermittelt wurden. Nicht vorgesehen ist dagegen eine strafbefreiende Wirkung einer solchen Selbstanzeige. Der Entwurf ist nach heftiger Kritik der Wirtschaft in der ablaufenden Legislaturperiode nicht in den Bundestag eingebracht worden. Das sollte Anlass sein, grundsätzlich über die rechtlichen Defizite der IT-Sicherheit nachzudenken.

## IT-Sicherheit: Die Gewohnheit des flächendeckenden Rechtsbruchs

Der Blick in die Praxis legt die Erkenntnis nahe, dass die übergroße Mehrheit aller Telemedienanbieter in der Praxis nichts an der umfassenden Protokollierung von IP-Nummern geändert hat und die bestehende Rechtslage souverän ignoriert.

Dies lässt sich auch empirisch belegen. Seit einigen Jahren untersucht die im Datenschutz-Auditing arbeitende Xamit Bewertungsgesellschaft jährlich in einem „Datenschutzbarometer“ jeweils einige tausend repräsentativ ausgewählte Webauftritte auf deren Einhaltung der Vorschriften des Telemedienrechts bei der Nutzerdaten-Protokollierung, den Datenschutzklauseln und anderen Regeln.[11] Xamit macht sich dabei den Umstand zunutze, dass zahlreiche Datenschutzverstöße und die programmtechnisch nötigen Vorkehrungen zum Einsatz von Protokollierungssoftware im Quellcode der jeweiligen Webangebote für jeden ablesbar und einfach dokumentierbar sind. Komplexere Verstöße läßt die Analyse unberücksichtigt.

Die Ergebnisse sind für den Datenschutz deprimierend: Von 2008 bis 2011 nahm die Zahl der offensichtlichen Datenschutzverstöße bei Unternehmen ebenso wie bei Behörden zu. Weniger als 10% der Webauftritte blieben 2008 ohne juristische Beanstandungen[12], in 2012 war das Ergebnis annähernd gleich: pro 100 Webauftritten seien 91 Beanstandungen durch Datenschutzbehörden auszusprechen.[13]

Die Datenschutzdebatte um Google Analytics 2012 verbesserte die Lage bei den Rechtsverstößen zur Nutzerdaten-Protokollierung leicht, was aber den Anstieg der restlichen Datenschutzverstöße nicht bremste. Die Autoren machten klar:

*„Wir sprechen hier nicht von den Verstößen, die einer unsicheren Rechtslage oder der Praxisferne des Bundesdatenschutzgesetzes geschuldet sind, sondern von den bewusst oder fahrlässig begangenen Verstößen“.*[14]

Es geht also um Rechtsbruch aus Gewohnheit. Die Wirklichkeit zeigt: So gut wie niemand schert sich um Recht und Gesetz in Sachen Datenschutz und IT-Sicherheit. So gut wie jeder protokolliert IP-Daten, was die Werkzeuge technisch gerade so hergeben. Und wenn es nutzt, werden auch Werkzeuge eingesetzt, die selbst für Laien offensichtlich rechtswidrig sind.

Und es bleibt folgenlos. Die von Beratungsunternehmen wie Xamit erhobenen und gesammelten Verstöße bei Unternehmen und Behörden werden von Datenschutzbehörden in den wenigsten Fällen geahndet. Mit dieser Untätigkeit gegenüber den ungebremsten und rechtswidrigen Datensammlungen untergraben sie allerdings selbst ihre Autorität. Auch wenn der Bundesbeauftragte für Datenschutz, Peter Schaar, nun zutreffend vor einer Gefahr warnt, eine rechtliche Regelung von Datensammlungen zu Zwecken der IT-Sicherheit könnte zu einer uferlosen Sammlung von Nutzerdaten führen[15], sollte man abwägen, den realen und flächendeckenden, rechtswidrigen Wildwuchs weiter zu ignorieren und zu belassen, oder der IT-Sicherheit einen rechtskonformen, legalen Weg zu bahnen.

## Rechtsfeste und praktikable Lösungsansätze

Als Lösung des Problems läge es daher nahe, die IP-Nummernprotokollierung bei Telemedien zu Zwecken der IT-Sicherheit zu regeln – und zwar möglichst eng begrenzt. Die letzte Novelle des BSI-Gesetzes hat dazu eine diskutable Vorlage geliefert. Diese ließe sich für eine Ergänzung des Telemediengesetzes anpassen. Die Alternative, die Regelung zur Protokollierung bei Telekommunikationsnetzen in §100 TKG, geht dagegen deutlich zu weit und erlaubt – übertragen auf IT-Sicherheitsaspekte im Internet – eine unnötig umfangreiche Datensammlung.

Ziel aus Sicht der IT-Sicherheit müsste es sein, eine Protokollierung von IP-Nummern und deren Nutzung klar zu regeln. Erlaubt ist heute die Auswertung der Verkehrsdaten im engen zeitlichen Bezug zu einer Webservice-Nutzung. Für die Praxis lässt sich daraus ein handhabbarer und datenschutzrechtlich tragbarer Ablauf aus drei Schritten entwik-

keln, der in vielen Teilen bereits Praxis ist:

1. Ein Intrusion Detection System kann aus den laufenden Verkehrsdaten eine Eingrenzung auf Verdachtsfälle leisten und den Rest der Daten verwerfen oder – ebenfalls legal – pseudonymisieren, etwa durch ein Verkürzen der IP-Nummern. Im Verdachtsfall ist unmittelbar ein auditierbares Verfahren zur Gefahrenanalyse und -abwehr anzuwenden.
2. Die systematische Analyse gespeicherter pseudonymisierter Protokolldaten, die ihrerseits nach einer überschaubaren Frist gelöscht werden, reicht auch über die Vorlaufzeit von größeren Angriffen aus, um eine Entscheidung über das Vorgehen bei vermuteten Angriffen zu treffen.
3. Als Ergebnis der Analyse sind nach überschaubarer Zeit entweder alle harmlosen pseudonymisierten Daten zu löschen oder es ist gezielt konkreten Verdachtsfällen nachzugehen, für die die Verkehrsdaten vollständig zu erfassen und in dem etablierten geordneten, auditierbaren Verfahren zu verarbeiten sind.

Das Bundesverfassungsgericht hat nach dem Grundrecht auf informationelle Selbstbestimmung das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ definiert. Die IT-Sicherheit ist das Arbeitsfeld, in dem der Schutz dieser beiden fundamentalen Grundrechte der Informationsgesellschaft praktisch umgesetzt werden muss. Der skizzierte Ablauf wäre eine einfache und professionell gut beherrschbare Lösung für die IT-Sicherheit, die den Anforderungen an Datenschutz und Sicherheit gerecht wird und für die nur wenig gesetzgeberische Arbeit für die Erlaubnis zur Speicherung der vollständigen IP-Nummern bei Verdacht und rechtliche Anforderungen an das Verfahren benötigt würde.

## Vergebliche Suche im IT-Sicherheitsgesetz

Der diskutierte Gesetzesentwurf des IT-Sicherheitsgesetzes sieht als Änderung am Telemediengesetz aber nur in Artikel 3 vor, den Diensteanbietern „Maßnahmen zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubten Zugriff“ nach dem Stand der Technik vorzuschreiben. Alles andere bleibt genauso ungeregelt wie bisher. Legal bliebe damit für die Zukunft beispielsweise das Betreiben von Intrusion Detection Systemen über Daten aus dem laufenden Betrieb und das Melden von Denial-of-Service-Attacken, solange ein Angriff andauert. Nicht legal aber bliebe das Detektieren eines Einschleusens von Trojanern und Botnetzen, oder jede andere, aus mehreren Schritten und verschiedenen „Nutzungsvorgängen“ bestehende Form eines Angriffs, für dessen Verfolgung detaillierte Daten verschiedener Nutzungsvorgänge zusammengeführt werden müssen. Nicht legal wird es selbstverständlich auch in Zukunft nicht sein, die IP-Kennung des Angreifers zu speichern.

Wer einige der Betreiber kritischer Infrastrukturen und ihre Herangehensweise an IT-Sicherheitsthemen kennt, weiß, dass dort zu diesem Thema, das nicht das Kernkompetenzfeld der Betreiber darstellt, vielfach ein defensives, rechtlich eher unzweifelhaftes Agieren einem Vorgehen vorgezogen wird, das letztlich auf einem systematischen Bruch des IT- und Datenschutzrechts aufbauen muss.

Man könnte dies aber auch anders formulieren: Die bekannt lückenhafte Rechtslage zur IT-Sicherheit ist selbstverständlich auch eine praktische juristische Argumentationsgrundlage, um jede Berichterstattung über IT-Sicherheitsvorfälle zu unterlassen, für deren Detektion es keine klare Rechtsgrundlage gibt. Da legal nur über eine begrenzte Anzahl möglicher Internet-basierter Angriffsformen überhaupt Daten gesammelt werden dürfen, ließe sich der Berichtsaufwand in überschaubaren Grenzen halten; Bußgelder oder andere Zwangsmaßnahmen stehen auch nicht zu befürchten. Dementsprechend unvollständig dürften die Lageberichte geraten, die das BSI aus den Meldungen der Betreiber kritischer Infrastrukturen zusammenstellen soll.

## Geld für Strafverfolgung statt für Datensammlungen

Was also sollte ein IT-Sicherheitsgesetz in der vorgelegten Form bringen? Die Kernforderung des Gesetzes – die Datensammlung von IT-Sicherheitsvorfällen – ist in der Fachcommunity heftig umstritten. So ist bekannt, dass 2010 ein einziges Botnet für ein Drittel des gesamten Spam-Aufkommens im Internet verantwortlich war. Was, so fragen die Fachleute, werde da eine Datensammlung an Neuem beitragen? Zwei Studien aus sehr unterschiedlichen Richtungen kommen zum gleichen Ergebnis.

Die Microsoft-Forscher Dinei Florencio und Cormac Herley publizierten 2011 eine qualitative Analyse der über Cybercrime publizierten Studien, Daten und Schadenshöhen. Ihr „harsches“ Ergebnis war, dass alle untersuchten Studien jeder belastbaren Datengrundlage entbehrten und überdies methodisch so grundlegend fehlerhaft seien, dass den Ergebnissen keinerlei Glaube geschenkt werden könne:

*„Our assessment of the quality of cyber-crime surveys is harsh: they are so compromised and biased that no faith whatever can be placed in their findings.“*[16]

Zum selben Resultat kam eine Studie britischer, deutscher, niederländischer und amerikanischer Wissenschaftler auf Initiative des britischen Verteidigungsministeriums. Auch ihre Schlussfolgerungen und Forderungen sind eindeutig:

*„The straightforward conclusion to draw on the basis of the comparative figures collected in this study is that we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.) but we should certainly spend an awful lot more on catching and punishing the perpetrators.“*[17]

Wenn keine der verfügbaren Datensammlungen über IT-Sicherheitsvorfälle irgendeinen objektiven Wert oder Nutzen hat, liegt die Frage nahe, ob und wenn ja, welche Abhilfe von der Sammlung von Sicherheitsvorfällen auf Basis eines IT-Sicherheitsgesetzes zu erwarten ist. Dass die betroffenen Unternehmen gute juristische Argumente haben, ihre Berichte schlank zu halten, ist offensichtlich.

Ausdrücklich kann und soll dies nicht bedeuten, dass Unternehmen, die IT-Sicherheitsvorfälle aus Gründen negativer Medienreaktionen verschweigen wollen, dies ungerührt weiter tun soll-

ten, weil ihnen die Veröffentlichung von Sicherheitslücken peinlich ist. Öffentlichkeit und die Benachrichtigung der Kunden solcher Unternehmen bei Sicherheitsvorfällen sind ein wichtiger Schritt, um Kunden – etwa im Fall des Diebstahls von Kreditkartendaten – eine schnelle Sperrung zu ermöglichen. Darum geht es im IT-Sicherheitsgesetz aber nicht.

Als der eigentliche Zweck des IT-Sicherheitsgesetzes erscheint vor allem, das Datenmaterial für einen alljährlichen Bericht zur Lage der IT-Sicherheit in ausgesuchten Bereichen zu sammeln und diesen Bericht pressewirksam vorzustellen. Die weltweit tätigen großen IT-Sicherheitsfirmen tun dies heute auch – und zwar durchaus mehrfach im Jahr. Diese Berichte sind unterhaltsam für die Medienberichterstattung, aber – wie gezeigt – leider fachlich ohne Substanz.

Was aber ist der Nutzen von Lageberichten zur IT-Sicherheit, die lükkenhaft, unsystematisch und in ihren Schlussfolgerungen verzerrt sind? Wie sehen die Maßnahmen und Aktionen aus, die aus solchen untauglichen Lageberichten abgeleitet und ergriffen werden? Wofür sollen schließlich private und öffentliche Gelder für eine Verbesserung von IT-Sicherheit eingesetzt werden, wenn diese auf untauglichen Lageanalysen beruhen?

Sollte der Zweck eines Gesetzes im Kern aber nur aus einem weiteren Bericht für die Medienberichterstattung bestehen, dessen Inhalt kein Experte vertrauen kann? Wäre es nicht eher nötig, der Verfolgung von Straftaten im IT-Bereich endlich eine rechtlich eindeutige Grundlage zu geben?

Die vielfach formulierte Forderung, das Geld nicht in Berichte, sondern in die Kompetenzentwicklung der Strafverfolger zu stecken, war immer die bessere, aber auch aufwändigere Idee. Die Bundesregierung legt sich selbst im neuen IT-Sicherheitsgesetz die Messlatte ein wenig höher: Dem Bundeskriminalamt sollen Zuständigkeiten für Computerkriminalität gegen Bundesbehörden übertragen werden. Begründung:

*„die Zuständigkeit für die polizeilichen Aufgaben der Strafverfolgung [liegt] in der Regel bei den Ländern, wobei die örtliche Zuständigkeit oftmals dem Zufall überlassen bleibt, abhängig davon, wo der Vorfall zuerst entdeckt wird.“*[18]

Und dort findet die zufällig veranlasste Ermittlungstätigkeit dann oft ihr schnelles Ende. Nun wäre die Bundesregierung zuständig für die nötige finanzielle und personelle Ausstattung – und damit die deutlich bessere Fachkunde – für polizeiliche Ermittlungsarbeit in Sachen IT. Der reale Wille zu Besserung ließe sich in Zukunft hier erkennen.

Die rechtlichen Befugnisse für die technische Ermittlung relevanter Daten für diverse Internet-basierte Straftaten aber hat das BKA auch in Zukunft nicht. Vielleicht ist es ja mit der Strafverfolgung gar nicht so ernst gemeint. Die „Cyberkriminellen“ dürfte das freuen. Der „Kampf gegen die Cyberkriminalität“ wird so jedenfalls nicht zu gewinnen sein.

Die Bürgerinnen und Bürger jedoch müssen auf den besseren Schutz wesentlicher Grundrechte in der Informationsgesellschaft wohl noch länger warten.

1 http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf

2 http://www.daten-speicherung.de/index.php/urteil-vorratsspeicherung-von-kommunikationsspuren-verboten/#lg

3 http://www.heise.de/newsticker/meldung/Mehrzahl-der-Bundesministerien-speichert-IP-Adressen-184012.html

4 Antwort der Bundesregierung, Bt.-Drs. 16/6938, Antwort auf Frage 11, http://dipbt.bundestag.de/dip21/btd/16/069/1606938.pdf

5 ebd. Frage 13

6 http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html

7 ebd. zu Nr. 122

8 Ebd., zu Nr. 161

9 Ebd. zu Nr. 174

10 Referentenentwurf des Bundesministeriums des Innern Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Stand 5.03.2013; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile

11 Eine Übersicht über die Studien unter: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php

12 Niels Lepperhoff, Björn Petersdorf: Datenschutz bei Webstatistiken; in: Datenschutz und Datensicherheit Nr. 4, 2008, S. 266-269

13 Xamit-Datenschutzbarometer 2012, a.a.O.

14 Xamit-Datenschutzbarometer 2012, S. 8; http://www.xamit-leistungen.de/downloads/Files.php?f=XamitDatenschutzbarometer2012.pdf

15 http://www.heise.de/newsticker/meldung/Datenschuetzer-Schaar-Plaene-zur-Abwehr-von-Cyber-Angriffen-bedenklich-1832914.html

16 Dinei Florencio, Cormac Herley: Sex, Lies and Cyber-crime Surveys, Redmont, Juni 2011, S. 8; http://research.microsoft.com/apps/pubs/default.aspx?id=149886 und http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf ,

17 Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage: Measuring the Cost of Cybercrime, S. 26. Paper zum Vortrag auf dem Workshop on the Economics of Information Security (WEIS), Berlin, 2012; http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

18 Begründung des IT-Sicherheitsgesetzes, S. 23

Karsten Neumann

# Live-Streaming von Gemeindevertretungssitzungen: Informationsrechte im Spannungsfeld datenschutzrechtlicher Anforderungen

**Das Internet entfaltet zunehmend auch seine Potentiale für mehr demokratische Selbst- und Mitbestimmung: dies gilt bis hin zur kleinsten Gemeinde. Unter den scheinbar gegensätzlichen gesetzlichen Zielbestimmungen Informationsfreiheit und Datenschutz wurden nicht nur in Mecklenburg-Vorpommern Vorhaben der Übertragung von Gemeindevertretersitzungen im Internet diskutiert und durch den Gesetzgeber mehr oder weniger überzeugend geregelt. Der Beitrag beleuchtet am Beispiel der Rechtslage in Mecklenburg-Vorpommern die Anforderungen an eine verfassungsrechtlich zulässige Satzungsregelung und die datenschutzrechtlich erforderlichen technisch-organisatorischen Maßnahmen.**

Das Recht der Bürger in Mecklenburg-Vorpommern auf freien Zugang zu allen bei der öffentlichen Hand vorhandenen Informationen soll die Voraussetzungen für eine demokratische Beteiligung der Öffentlichkeit an allen Entscheidungsprozessen stärken. Dafür braucht es den Zugang der Bürgerinnen und Bürger zu Informationen. Diesen Anspruch schafft und gestaltet das Gesetz zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern seit dem 11. Juli 2011. Auch beim Datenschutz geht es um viel mehr, als um Daten: Ziel der Datenschutzvorschriften ist es, das Recht des Einzelnen zu schützen, aus eigener Selbstbestimmung sein Leben zu planen, Entscheidungen zu treffen oder Chancen wahrzunehmen. Das Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz – DSG MV) gewährleistet bereits seit 1992 die Umsetzung des Verfassungsanspruchs auf informationelle Selbstbestimmung auch in und durch die Landes- und Kommunalverwaltung.

Bei einem Konflikt beider Rechtsansprüche ist ein Ausgleich erforderlich, für den die Gesetze Maßstäbe bereithalten. Gerade in der Arbeit der kommunalen Vertretungen sind die Abgeordneten im Rahmen ihrer Verantwortung für das Gemeinwohl mit vielen unterschiedlichen, oft sehr persönlichen Informationen konfrontiert. Zugleich findet ein Großteil der Arbeit der Kommunalvertretungen zu Recht in der Öffentlichkeit statt. Die öffentliche Kontrolle der Tätigkeit schließt aber den Schutz der berechtigten Interessen der Betroffenen nicht aus. Vielmehr ist die Summe der Einzelinteressen ein wichtiger Teil des Gemeinwohlinteresses. Das Informationsfreiheitsrecht verlangt diesen Interessenausgleich und gibt deshalb klare Regeln zum Vorrang datenschutzrechtlicher Schutzansprüche vor, bei deren Berücksichtigung der respektvolle Umgang miteinander möglich sein sollte.

Seit dem Jahr 2012 beschäftigen sich viele Gemeindevertretungen auf der Grundlage von parlamentarischen Initiativen verschiedener Parteien mit der Einführung der Live-Übertragung der öffentlichen Sitzungen der Gemeindevertretungen über das Internet als einer sehr kostengünstigen Möglichkeit der Stärkung direkter Bürgerbeteiligung durch eine unmittelbare Informationsmöglichkeit für Jedermann. Das IFG M-V gewährt jedoch nur einen verwaltungsverfahrensrechtlichen Zugang zu vorliegenden Informationen für den direkt Betroffenen. Die Stärkung demokratische Beteiligungsrechte ist zwar intendiert, aber nicht reguliert. Damit scheidet das IFG M-V zwar als Rechtsgrundlage aus, gibt aber sehr wohl als landesgesetzgeberische Stellungnahme Hinweise auf bewährte und zwischenzeitlich umfänglich wissenschaftlich evaluierte[1] Lösungsstrategien. Die kommunalen Bemühungen für mehr Transparenz stießen und stoßen auf mehr oder weniger Widerstand – auch mit datenschutzrechtlichen Bedenken begründet.

## Datenschutzrecht anwendbar?

Das sog. Live-Streaming beschreibt eine Technologie zur Übertragung von Videobildern und Ton in Echtzeit über das Internet. Diese Angebote werden oft mit einem „On-Demand"-Streaming verknüpft, bei dem die Live-Daten gespeichert und zu einem späteren Abruf bereitgehalten werden. Aber auch ohne eine solche Verknüpfung muss bei einer Übertragung ins Internet immer von einer langfristigen Speicherung der so veröffentlichten Daten ausgegangen werden. Wird der Stream einmal zum Abruf bereitgehalten, muss man davon ausgehen, dass diese Bilder auch durch Nutzer gespeichert werden. Der Abruf durch anfragende Rechner und deren Verwendung der Daten entzieht sich mit der einmal erfolgten Abrufmöglichkeit jeder Kontrollmöglichkeit des Anbieters. Weder kann eine Aufzeichnung technisch verhindert, noch einmal Veröffentlichtes nachträglich wieder gelöscht werden.

Beim Live-Streaming kann diese Datenübertragung entweder direkt durch den Videoproduzenten (Peer-to-peer), oder durch eine Server-basierte Übertragung erfolgen. Letztere sind inzwischen weiter verbreitet. Hierfür gibt es eine Fülle inzwischen preisgünstiger Angebote, wobei vor allem die Anzahl gewünschter gleichzeitiger Zugriffsmöglichkeiten preisbildend ist.

Mit rund acht Millionen Zuschauern war der Stratosphären-Sprung des Extremsportlers Baumgartner der bisher meistgesehene Videostream. Die technischen Voraussetzungen für ein Live-Stream sind also mit der erforderlichen Videotechnik sowie der Datenübertragung zu einem Server relativ einfach überall und jederzeit herzustellen.

Jede Erhebung, Verarbeitung oder Übermittlung personenbezogener Daten ist von Verfassung wegen nur dann zulässig, wenn ein Gesetz diese erlaubt und konkrete Anforderungen an den Schutz dieser Daten vor einem möglichen Missbrauch festlegt.[2] Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person – so die juristische Definition. Diese Definition des Personenbezugs geht bewusst so weit, weil die wesentliche Besonderheit der elektronischen Datenverarbeitung darin besteht, dass elektronische Daten unbemerkt kopiert, weitergegeben, ausgelesen und mit anderen Informationen verknüpft werden können. Ein Schutz vor möglichem Missbrauch kann also nur gelingen, wenn die Daten von Anfang an gegen jegliche nur denkbare weitere zweckwidrige Verwendung geschützt werden.

Das bedeutet jedoch nicht, dass damit die Verwendung solcher Daten verboten sei. Vielmehr führt die Anwendbarkeit des Datenschutzrechtes zu einer genaueren Prüfung der Zulässigkeit und einer Festlegung von Bedingungen der Verarbeitung.

Dabei wird nach deutschem Datenschutzrecht generell zwischen der Datenverarbeitung durch öffentliche Stelle – dann sind die Landesdatenschutzgesetze bzw. das Bundesdatenschutzgesetz mit seinen Regelungen für öffentliche Stellen des Bundes anzuwenden – und die durch nicht-öffentliche Stellen – dann ist das Bundesdatenschutzgesetz anzuwenden – unterschieden. Verantwortlich im Sinne des Datenschutzrechtes ist immer diejenige Stelle, in deren Auftrag (zur Erfüllung deren Zwecke) die Datenverarbeitung erfolgt.

Soll also das Live-Streaming durch die Gemeinde selbst oder in deren Auftrag durch einen Privaten (Stadtfernsehen oder IT-Dienstleister) erfolgen, ist das Landesdatenschutzrecht anwendbar. Erfolgt hingegen das Live-Streaming durch einen Dritten im eigenen Interesse, bestimmt sich die Zulässigkeit nach den Regeln für nicht-öffentliche Stellen nach dem Bundesdatenschutzgesetz.

## Live-Streaming durch die Gemeinde

Das Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz – DSG MV) gilt gem. § 2 „für Behörden und öffentlich-rechtliche Einrichtungen und Stellen des Landes, der Gemeinden, der Ämter, der Landkreise sowie für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts (öffentliche Stellen).“ Nur „soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor“, § 2 Abs. 4 DSG MV. Besondere Rechtsvorschriften in diesem Sinne können zum Beispiel Vorschriften der Kommunalverfassung MV sein, wenn und soweit diese den Umgang mit solchen Daten spezieller regeln.

Aufgezeichnete Videobilder gehören ebenso zu den personenbezogenen Daten, wie Tonaufnahmen. Die elektronische Aufzeichnung von Videobildern natürlicher Personen stellt eine automatisierte Verarbeitung personenbezogener Daten dar. Die Bilder, die im Kontext einer bestimmten Veranstaltung stehen, sowie die Sprachaufzeichnungen aus einer Gemeindevertretersitzung können bestimmten Personen zugeordnet werden, sind also zumindest personenbeziehbar. Da diese Bilder technisch bedingt – auch bei einer „live“-Übertragung – elektronisch gespeichert und verarbeitet werden, ist das Datenschutzrecht zur Anwendung zu bringen.

Das Erheben von personenbezogenen Daten bedeutet einerseits den konkreten Vorgang der Aufzeichnung der Video- oder Tondaten, aber auch die Abfrage der IP-Adressen von Nutzern des Live-Streaming-Angebotes durch den jeweiligen Server, der die Daten dann an den anfragenden Rechner übermittelt. Auch die IP-Adressen (Internet-Protokoll-Adressen, die jeweils in der Regel einem bestimmten Rechner zugeordnet werden können) sind personenbezogene Daten, solange sich aufgrund einer permanenten oder nur vorübergehenden Speicherung der Verbindungsdaten der Bezug zu einem konkreten Rechner herstellen lässt.

Wenn Daten an jemanden außerhalb der eigenen Behörde oder des eigenen Unternehmens weitergeleitet werden, findet eine Datenübermittlung statt. Damit ist also auch jede Art der Veröffentlichung eine Übermittlung, z.B. die weltweite Verbreitung mündlicher Beiträge in einer Sitzung der Gemeindevertretung.

Damit einhergehen mithin alle besonderen Gefahren für das Recht auf informationelle Selbstbestimmung durch die Nutzung des Mediums Internet.[3] So ist eine nachträgliche Löschung selbst bei einer unzulässigen Datenübertragung technisch jedenfalls bisher unmöglich.[4]

## Live-Streaming durch Dritte: Medien

Mit dem Gesetz über die Kommunalverfassung und zur Änderung weiterer kommunalrechtlicher Vorschriften vom 13. Juli 2011 (GVOBl. M-V. S. 777) wurde die Kommunalverfassung in § 29 Absatz 5 um eine Regelung zu Film- und Tonaufnahmen während der Sitzungen der Gemeindevertretungen und des Kreistages wie folgt ergänzt: „Die Sitzungen der Gemeindevertretung sind öffentlich. Die Öffentlichkeit ist auszuschließen, wenn überwiegende Belange des öffentlichen Wohls oder berechtigte Interessen Einzelner es erfordern. Der Ausschluss der Öffentlichkeit kann in diesem Rahmen in der Hauptsatzung oder durch Beschluss der Gemeindevertretung angeordnet werden. Über den Ausschluss der Öffentlichkeit wird in nichtöffentlicher Sitzung beraten und mit der Mehrheit aller Mitglieder der Gemeindevertretung entschieden. In öffentlichen Sitzungen der Gemeindevertretung sind Film- und Tonaufnahmen durch die Medien zulässig, soweit dem nicht ein Viertel aller Mitglieder der Gemeindevertretung in geheimer Abstimmung widerspricht.“

Die Kommunalverfassung definiert Umfang und Ausgestaltung der Sitzungsöffentlichkeit als Ausdruck des

Grundrechtes auf Informationsfreiheit nach Art. 5 Abs. 1 Satz 1 GG, soweit nicht Gründe des öffentlichen Wohl oder berechtigte Interessen Einzelner entgegenstehen. Der Grundsatz der Sitzungsöffentlichkeit entspricht dem allgemeinen Öffentlichkeitprinzip der Demokratie. Dieser ist allerdings hier nur analog anwendbar, da es sich bei der Gemeindevertretung rechtlich nicht um eine Parlament handelt, sondern diese als Kollegialorgan der Selbstverwaltung Teil der Exekutive ist[5], § 22 Abs. 1 KV MV. Der Zweck des Öffentlichkeitsprinzips, die staatlichen Entscheidungen einer direkten Kontrolle durch die Bürger zu unterziehen, wird bereits durch eine Vielzahl von gesetzlichen Maßgaben gesichert. Hierzu gehört die Sitzungsöffentlichkeit, die Bekanntgabe von Tagungsort und Tagesordnung, die Verschaffung einer Teilnahmemöglichkeit für Zuhörer oder die Bekanntgabe von Beschlüssen und Veröffentlichung von Protokollen. Die Zugänglichkeit in Form einer Saalöffentlichkeit – also des ungehinderten persönlichen Zugangs zur Sitzung – genügt nach heutiger Rechtsprechung zur Medienöffentlichkeit in Gerichtsverhandlungen[6] bereits den Anforderungen demokratischer Kontrolle.

Im politischen Diskurs wird dies in Anbetracht wachsender Wahlmüdigkeit, zunehmender Komplexität politischer Entscheidungen und einem sich wandelnden Mediennutzungsverhalten zu Recht kritisch gesehen. Die Bereitstellung von Informationen über das Internet bietet einer größeren Breite von Bürgerinnen und Bürgern die Möglichkeit der unmittelbaren Teilnahme an Diskussionsprozessen und dies auch zeitlich versetzt.

Einen Rechtsanspruch auf die Teilnahme an Sitzungen durch ein Live-Streaming-Angebot gibt es jedoch nicht, ebenso keinen Rechtsanspruch für Sitzungsteilnehmer zur Aufzeichnung.

Die Entscheidung obliegt dem jeweiligen Gesetzgebers und nach der Kommunalverfassung MV innerhalb des gesetzliche Zulässigen der Gemeindevertretung. Der Landesgesetzgeber hat in zulässiger Weise den Zugang zur Sitzung und die Möglichkeit der medialen Berichterstattung in der Kommunalverfassung MV 2011 neu geregelt.

Diese Neuregelung begründet die Landesregierung wie folgt: „Durch die Neuregelung zur Zulässigkeit von Filmaufnahmen und Tonmitschnitten in Absatz 5 wird es erstmals rechtssicher möglich, dem Informationsbedürfnis der Bürgerinnen und Bürger nach unmittelbarer Bild- und Tonberichterstattung durch die Medien Rechnung zu tragen. Aufgrund der bisherigen Rechtsprechung, die die Bereitschaft bzw. die Fähigkeit zur freien unvoreingenommenen Rede durch Film- und Tonaufnahmen gefährdet sieht, ist es bisher selbst im Falle des Einverständnisses sämtlicher Mandatsträger rechtlich umstritten gewesen, ob den Medien diese Art der Berichterstattung gestattet werden kann. Die Neuregelung verbessert die Transparenz des Sitzungsgeschehens gegenüber der Öffentlichkeit, gewährleistet aber auch einen Minderheitenschutz.“ [7]

Damit enthält die Kommunalverfassung eine spezialgesetzliche Regelung zu Bild- und Tonaufnahmen durch die Medien. „Medien“ bezeichnet dabei den Kreis der durch die Rundfunkfreiheit Art. 5 Abs. 1 Satz 2 GG besonders privilegierten Rundfunkveranstalter. Die zulässige Privilegierung der institutionalisierten Medien ist verfassungsrechtlich einerseits geboten, andererseits auch rundfunkrechtlich reglementiert.

Art. 5 Abs. 1 Satz 2 GG schützt die Freiheit der Berichterstattung als Funktionsgarantie des demokratischen Gemeinwesens. Dieser Schutz erstreckt sich auf den ungehinderten Zugang zur Gemeindevertretungssitzung und „die Möglichkeit, ein Ereignis den Zuhörern und Zuschauern unter Einsatz von Aufnahme- und Übertragungsgeräten akustisch und optisch in voller Länge oder in Ausschnitten, zeitgleich oder zeitversetzt zu übertragen.[8] In welcher konkreten technischen Ausgestaltung dies erfolgt, also auch ob als Live-Stream oder Aufzeichnung, unterfällt allein der Entscheidung des Rundfunkveranstalters bzw. den rundfunkrechtlichen Beschränkungen für die Internetpräsentation von Inhalten. Über die Zugänglichkeit und die Art des Zugangs entscheidet jedoch der jeweils Berechtigte in den Grenzen der gesetzlichen Vorgaben. Aus dem Grundrecht der Rundfunkfreiheit leitet sich ebenso wie aus dem Grundrecht auf Informationsfreiheit kein Zugangsanspruch ab, sondern allein der Anspruch auf einen diskriminierungsfreien Zugang.

## Live-Streaming durch sonstige Dritte

Die Kommunalverfassung enthält somit zwar eine vorrangige spezialgesetzliche Regelung für Medien, nicht jedoch für sonstige Dritte. Angesichts der Miniaturisierung der Aufnahme- und Übertragungstechnik wird es für die Sitzungsteilnehmer zunehmend schwieriger überhaupt zu erkennen, ob eine Aufzeichnung durch Ditte stattfindet und diese eventuell auch direkt ins Internet übertragen wird. Hier stößt das Datenschutzrecht mit fortschreitender technischer Entwicklung zunehmend an die Grenzen seiner Durchsetzbarkeit und damit seiner Legitimation. Die gleiche Problematik stellt sich für die Durchsetzbarkeit des Rechtes am eigenen Bild nach dem Kunsturhebergesetz.[9] Gleichwohl bleibt die Gemeindevertretung im Rahmen ihres Hausrechtes verpflichtet, während der Sitzung für die Wahrung der Rechte der Abgeordneten und der beteiligten Bürgerinnen und Bürger im Rahmen ihrer Möglichkeiten Sorge zu tragen. Dazu gehört auch die Durchsetzung des Rechtes auf informationelle Selbstbestimmung.

Die Gesetzesbegründung der Landesregierung zur Novellierung der Kommunalverfassung MV 2011 führt hierzu aus: „Soweit die Hauptsatzung neben den Medien auch Dritten mit berechtigten Interessen – bspw. Bürgerinitiativen – Film- oder Tonaufnahmen gestatten will, steht dem die gesetzliche Regelung nicht entgegen.“

Damit betont einerseits die Landesregierung die Nicht-Geltung der Sonderregelung für Medien für andere Dritte. Zugleich unterstreicht dies das Recht der Gemeindevertretung, den gleichen Sachverhalt bezüglich einer Übertragung durch Dritte selbst zu regeln. Dabei hat die Landesregierung allerdings unberücksichtigt gelassen (jedenfalls nicht hinzugefügt), ob bei einer solchen Gestattung gegenüber Dritten die gleichen Einschränkungen wie für Medien gelten sollen, also die pflichtige Untersagung, wenn dem ein Viertel aller Mitglieder der Gemeindevertretung in geheimer Abstimmung widerspricht.

Da die Gestattung selbst jedoch bereits Gegenstand einer Beschlussfassung der Gemeindevertretung ist und eine entsprechende Regelung in der Hauptsatzung der Gemeinde voraussetzt, ist eine vergleichbare verfahrensrechtliche Sicherstellung auch gegenüber Dritten durchsetzbar und zum Schutz der Minderheitenrechte auch geboten.

## Einschränkung der Übertragung durch Beschluss

Mit der Entscheidung zu § 29 Abs. 5 Satz 5 KV MV hat der Gesetzgeber den Zugang der Medien zu den dort genannten Bedingungen eröffnet. Dieser kann durch die Gemeindevertretungen nur aufgrund eines Beschlusses verwehrt werden, bei dem ein Viertel der Gemeindevertreter widersprechen. Zum Schutz der Entscheidungsfreiheit des einzelnen Abgeordneten sieht die Kommunalverfassung hierfür eine geheime Abstimmung vor. Dieses Verfahren entspricht nicht der Abstimmung zur Frage der Herstellung der Nicht-Öffentlichkeit einer Sitzung gem. § 29 Abs. 5 Satz 2 KV MV, die in nicht-öffentlicher Sitzung zu erfolgen hat, jedoch ohne das Erfordernis eines objektiven Geheimhaltungsgrundes und mit einem geringerem Quorum. Eine geheime Abstimmung ist jedoch teilweise aufwändiger, muss diese doch wie eine Wahlhandlung schriftlich erfolgen, um die Geheimhaltung trotz Sitzungsöffentlichkeit zu gewährleisten.

Die Wahl des Quorums von einem Viertel der Gemeindevertreter hat der Gesetzgeber nicht begründet, allerdings ein typisches Minderheiten-Quorum genutzt (so auch in §§ 29 As. 7, 31 Abs. 2, 34 Abs. 2, 37 Abs. 2, 71 Abs. 4 KV MV, dort allerdings in der Regel zusätzlich mit dem Quorum „oder eine Fraktion“). Andererseits verzichtete der Gesetzgeber auf die Möglichkeit, bereits den Widerspruch eines Einzelnen ausreichen zu lassen und macht damit deutlich, mit dieser Regelung nicht das individuelle Grundschutzbedürfnis eines Einzelnen im Auge gehabt zu haben, sondern einen eher politischen „Minderheitenschutz“. Damit entschied sich der Landtag ausdrücklich gegen die Empfehlung des Landesdatenschutzbeauftragten, hier das individuelle Selbstbestimmungsrecht eines Abgeordneten zu berücksichtigen. Eine schlüssige Begründung für das gewählte Quorum ergibt sich aus der Begründung des Gesetzentwurfes nicht. Insofern dürfte eine Prüfung der Verfassungsmäßigkeit dieser Regelung interessante Debatten auslösen.

Gleichwohl muss man diese Ausnahmeregelung auch bei der Gewährung der Möglichkeit des Live-Streamings für Dritte, die keine Medien im rechtlichen Sinne vertreten, oder bei einem Streaming durch die Gemeindevertretung selbst analog anwenden. Es ist kein Grund erkennbar, warum eine Veröffentlichung durch die Medien anders bewertet werden soll als eine Veröffentlichung durch Dritte auf einem Medium mit größerer und längerer Reichweite, dem Internet. Wenn man die Möglichkeit der Beeinträchtigung von Minderheitsrechten durch eine Übertragung von Debatten über das Internet überhaupt annimmt, dann unterscheidet sich diese jedenfalls kaum durch den jeweiligen Veranlasser. Ganz im Gegenteil darf man davon ausgehen, dass die Verbreitung professioneller Medien auch im Internet regelmäßig größer ist, als durch sonstige Dritte.

## Zugang durch Dritte nicht nur mit „berechtigtem Interesse“

In der Gesetzesbegründung nimmt der Gesetzgeber die Möglichkeit einer Berichterstattung durch Dritte in der Weise auf, dass der Gemeindevertretung durch eine Regelung in der Hauptsatzung damit weiterhin die Möglichkeit eröffnet sei, auch Dritten „mit berechtigten Interessen“ Film- oder Tonaufnahmen zu gestatten.

Offen lässt der Gesetzgeber, wie zwischen Dritten mit und ohne „berechtigtem Interesse“ unterschieden werden soll. Da eine solche Unterscheidung gesetzlich nicht vorgesehen ist, sollte hierauf aus Praktikabilitätserwägungen bei der Ausgestaltung einer Hauptsatzungsregelung verzichtet werden. Eine Unterscheidung zwischen berechtigtem und unberechtigtem Interesse würde jeden Entscheider dem Vorwurf einer Zensur aussetzen und wäre gerichtlich auch nicht überzeugend überprüfbar. Da ein rechtliches Interesse im Sinne eines Rechtsanspruches für Dritte in der Regel ausscheidet, bietet sich hier in Analogie zum Informationsanspruch aus dem Informationsfreiheitgesetz allein eine Gleichbehandlung an. Sollten sich zu viele Fernsehteams oder sonstige Videokameras im Sitzungssaal befinden und dadurch den Verlauf der Sitzung oder die mit gleichen Rechten ausgestatteten sonstigen Zuhörer stören, kann hierauf im Einzelfall mit den Mittel des Hausrechtes reagiert werden. Hier kann in Anlehnung an die Erfahrungen bei Gerichtsverhandlungen eine Akkreditierung bzw. vorherige Anmeldung verlangt werden, der Zutritt auf einen bestimmten Bereich räumlich oder zeitlich begrenzt werden oder Vorgaben zur Kameraführung und Ausleuchtung gemacht werden.

## Hauptsatzung als Rechtsgrundlage

Eine „andere Rechtsvorschrift“ gem. § 7 Abs. 1 Nr. 2 DSG MV kann neben einem bereichsspezifischen Gesetz wie der Kommunalverfassung auch eine Satzung der Körperschaft sein. „Wie die staatlichen Gesetzgeber für ihren Kompetenzbereich gehalten sind, normenklare bereichsspezifische Grundlagen für die Datenverarbeitung zu schaffen, müssen dies auch Satzungsgeber im Rahmen ihrer Zuständigkeit. Satzungen haben deshalb ausdrücklich die notwendigen und zulässigen Verarbeitungsschritte zu benennen und festzulegen, von wem, auf welche Weise und für welche Aufgaben die erforderlichen personenbezogenen Daten verarbeitet werden dürfen.“[10]

Sollte es im Rahmen der Aufgabenerfüllung der Gemeindevertretung im Einzelfall erforderlich sein, auf die persönlichen oder sachlichen Verhältnisse eines Bürgers derart einzugehen, dass hierbei konkrete Einzelangaben über bestimmte oder bestimmbare Personen in einer öffentlichen Sitzungen offenbart werden, richtet sich die Beurteilung einer solchen Übermittlung – im Sinne einer Bekanntgabe an Dritte – nach §§ 7 Abs.1 Nr. 1, 10 Abs. 1 DSG.

Während des Live-Streamings einer Gemeindevertretungssitzung werden einerseits die Äußerungen, das Abstimmungsverhalten oder auch das nonverbale Verhalten eines Abgeordneten übermittelt. Diese Übermittlung soll

dem Zweck dienen, die demokratische Beteiligungsmöglichkeit der Bevölkerung, die Informiertheit über den demokratischen Prozess und nicht zuletzt damit die Akzeptanz von Entscheidungen zu verbessern. Diese Zielstellung geht über eine bloße Öffentlichkeitsarbeit hinaus, braucht es doch hierfür Glaubwürdigkeit durch Authentizität.

Gem. § 22 KV MV ist die Gemeindevertretung die Vertretung der Bürgerinnen und Bürger und das oberste Willensbildungs- und Beschlussorgan der Gemeinde. Ihre Mitglieder üben ihr Mandat im Rahmen der Gesetze nach ihrer freien, nur dem Gemeinwohl verpflichteten Überzeugung aus. Sie sind an Aufträge und Verpflichtungen, durch welche die Freiheit ihrer Entschließungen beschränkt wird, nicht gebunden. Die Mitglieder der Gemeindevertretung sind zur Teilnahme an den Sitzungen und zur Mitarbeit verpflichtet, wenn sie nicht aus wichtigem Grund verhindert sind (§ 23 KV MV). Gemäß § 29 Abs. 5 KV MV sind die Gemeindevertretungssitzungen öffentlich.

Obwohl die Gemeindevertretung kein Parlament im verfassungsrechtlichen Sinne ist, sondern als Organ der Gemeinde neben dem Organ Bürgermeister steht, erfüllt sie ihre Aufgaben in der Regel als demokratisches Organ in der und kontrolliert durch die Öffentlichkeit. Ihre Mitglieder werden in demokratischen Wahlen bestimmt und müssen sich damit auch einer demokratischen Öffentlichkeit stellen.

Allerdings enthält die Kommunalverfassung zwar Regelungen zu den Aufgaben, zur Gestaltung des Sitzungsablaufes und zum Zugang der Öffentlichkeit hierzu, aber keine den verfassungsrechtlichen Anforderungen an Normenklarheit genügende Datenverarbeitungsgrundlage. Damit scheidet die Kommunalverfassung als mögliche Rechtsgrundlage aus.

Will die Gemeindevertretung selbst ihre öffentlichen Sitzungen zur Förderung der demokratischen Beteiligung und Information der Bürgerinnen und Bürger über das Medium Internet breiteren Kreisen der Bevölkerung zugänglich machen, braucht sie hierfür gem. § 7 Abs. 1 Nr. 2 DSG MV eine Rechtsgrundlage. Da die Kommunalverfassung keine normenklare gesetzliche Grundlage für die Verarbeitung personenbezogener Daten zur Öffentlichkeitsarbeit enthält, ist eine Regelung in der Hauptsatzung erforderlich.

Die Hauptsatzung kann eine gesetzliche Grundlage im Sinne des DSG MV sein[11], wenn diese hinreichend normenklar und verhältnismäßig die Datenverarbeitung gestattet, also ihrerseits die verfassungsrechtlichen Anforderungen aus der Grundrechtsausprägung des Rechtes auf informationelle Selbstbestimmung erfüllt[12].

Die Gemeinde hat im Rahmen der verfassungsrechtlich garantierten Selbstverwaltung und im Rahmen der Gesetze ein Satzungsrecht, § 5 Abs. 1 KV MV. Hierüber kann die Gemeindevertretung zusätzlich zum Recht der Medien auf Berichterstattung gem. § 29 Abs. 5 KV MV selbst zu der Entscheidung kommen, ein Live-Streaming für erforderlich zur Erfüllung der Aufgaben der Gemeindevertretung anzusehen und damit auch die datenschutzrechtliche Grundlage durch Satzungsregelung schaffen. Rechtmäßig zustande gekommene Satzungen können eine Rechtsgrundlage für Datenverarbeitungen im Sinne des § 7 Abs. 1 Nr. 2 DSG MV sein. Hieraus folgt das zwingende Erfordernis der Schaffung einer Regelung, in der die wesentlichen Anforderungen und Bedingungen transparent, normenklar und verhältnismäßig geregelt sind.

## Regelungsinhalt der Satzung

Die Hauptsatzungsregelung sollte in der Zweckbestimmung der Live-Streaming-Gestattung an die Aufgaben der Gemeindevertretung anknüpfen und die Erlaubnis auf diese Zwecke begrenzen. Zusätzlich sollte der Umfang genau bestimmt werden. Hier kann ein Unterschied zwischen den Sitzungen der Gemeindevertretung und den Ausschüssen gemacht werden. Daneben ist es empfehlenswert, auch die Dauer des Bereithaltens einer Aufzeichnung festzulegen. Hier kann die Gemeindevertretung je nach Zielrichtung der Aufzeichnung variieren. Auch wenn eine solche Beschränkung keine Gewähr dafür bietet, dass Aufzeichnungen nicht auch zu einem späteren Zeitpunkt noch online verfügbar sind, könnte die Maßnahme geeignet sein, einer dauernden Verfügbarkeit entgegen zu wirken. Soll nur eine zeitnahe Nachvollziehbarkeit der Beratungen der Gemeindevertretung ermöglicht werden, wäre eine Beschränkung auf sieben Tage im Anschluss der Gemeindevertretungssitzung denkbar, wie es aus anderen Gründen für öffentlich-rechtliche Medieninhalte vorgeschrieben ist. Maßstab könnte aber auch eine Wahlperiode oder wenigstens ein Jahr sein, um auch die Nachverfolgbarkeit bestimmter kommunalpolitischer Entscheidungen zu ermöglichen.

Diese Regelung könnte wie folgt ausgestaltet sein:

- E(1) Die öffentlichen Sitzungen der Gemeindevertretung und ihrer Ausschüsse werden zur Förderung der demokratischen Beteiligung der Bürger durch die Gemeinde live im Internet übertragen und als Aufzeichnung für den Zeitraum von … zum Abruf über die Internetseite der Gemeinde bereit gehalten.
- E(2) Die Übertragung kann auch durch Dritte erfolgen. Ein Anspruch hierauf besteht nicht.

Soweit eine Datenverarbeitung grundsätzlich zulässig sein soll, ist die Wahrnehmung der Betroffenenrechte sicher zu stellen. Dies gilt sowohl bei der Durchführung des Live-Streamings durch die Gemeinde selbst als auch bei der Durchführung durch Dritte.

Von einer Datenverarbeitung betroffen sind alle Personen, von denen Daten in diesem Zusammenhang verarbeitet werden. Für ein Live-Streaming während einer Gemeindevertretungssitzung kommen folgende Betroffenengruppen in Betracht:

- die gewählten Gemeindevertreter,
- berufene oder sachkundige Ausschussmitglieder, die nicht Mitglieder der Gemeindevertretung sind,
- Beschäftigte der Gemeinde,
- Personen, deren Daten zum Gegenstand der Beratung gemacht werden,
- Bürger, die die Möglichkeit einer Bürgeranfrage nutzen wollen und
- Zuhörer.

Zu den jeweiligen Betroffenengruppen sind neben den allgemeinen Rechten

auch spezifische Vorschriften zu berücksichtigen.

So ist bei einer möglichen Einbeziehung von Beschäftigten der Gemeinde in die Berichterstattung der Personalrat rechtzeitig einzubeziehen. Dieser hat im Rahmen seines Überwachungsrechts die Befugnis, bei dem Dienststellenleiter auf die Beachtung der Datenschutzrechte der Mitarbeiter hinzuwirken.[13] Der Bürgermeister selbst muss dann diese Verantwortung auch gegenüber der Gemeindevertretung geltend machen und notfalls durchsetzen.

Soweit personenbezogene Daten zum Gegenstand einer Beratung der Gemeindevertretung gemacht werden sollen oder müssen, ist die Öffentlichkeit und damit auch das Live-Streaming grundsätzlich auszuschließen.

Da der Umstand der Live-Berichterstattung geeignet ist, das Recht auf eine Bürgeranfrage während der Sitzung einzuschränken, ist die Möglichkeit der Einschränkung der Übertragungsrechte im Einzelfall in die Hauptsatzung aufzunehmen. Bürgerinnen und Bürger könnten die im Gegensatz zur Sitzungsöffentlichkeit potentiell deutlich erweiterte Öffentlichkeit und vor allem den Umstand einer jederzeit möglichen Aufzeichnung, Speicherung und Widergabe von einer Fragestellung abhalten.

Hierauf sollte die Gemeindevertretung Rücksicht nehmen und den Fragestellern entweder das Recht einräumen, selbst zu entscheiden und die Unterbrechung der Übertragung zu verlangen, oder organisatorisch sicher stellen, dass die Personen nicht gezeigt werden, sondern nur die Beantwortung.

Eine entsprechende Satzungsregelung könnte wie folgt ausgestaltet sein:

- E(3) Das Live-Streaming erfolgt ausschließlich durch Aufzeichnen eines Bildes des Rednerpultes und des Präsidiums der Gemeindevertretung. Bürgeranfragen dürfen nur als Ton aufgezeichnet werden.

.

Verantwortlich für den rechtmäßigen Umgang mit den personenbezogenen Daten ist die so genannte „Daten verarbeitende Stelle“. Dabei gilt das Landesdatenschutzgesetz für Behörden und öffentlich-rechtliche Einrichtungen und Stellen des Landes, der Gemeinden, der Ämter, der Landkreise sowie für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts (öffentliche Stellen) sowie für juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die dieses Gesetz Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet das DSG MV auch dort entsprechende Anwendung. Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

Besondere Anforderungen ergeben sich dann, wenn die zuständige Stelle einen Dritten mit der Verarbeitung personenbezogener Daten beauftragt, der sog. Auftragsdatenverarbeitung. Auch bei der Beauftragung Dritter bleibt die Behörde datenschutzrechtlich verantwortlich, die den Auftrag erteilt, § 4 Abs. 1 DSG MV. Daraus folgt die Anforderung, beim Auftragnehmer den gleichen Sicherheitsstandard für die personenbezogenen Daten der Betroffenen zu gewährleisten, wie er innerhalb der Behörde wäre. Dies beginnt bereits bei der Auswahl eines geeigneten Auftragnehmers, der seine Eignung vor der Vergabe des Auftrages nachweisen muss. Dabei reicht es nicht aus, sich auf Erklärungen zu verlassen. Vielmehr müssen alle Details der Datenverarbeitung und deren Randbedingungen vertraglich geklärt und vorab sowie dann laufend vor Ort geprüft werden. Die konkreten Anforderungen hierfür ergeben sich aus dem Gesetz.

Es ist nur ein scheinbarer Widerspruch, wenn das Datenschutzrecht einen Transparenzgrundsatz hat. Dieser Grundsatz ist vielmehr die logische Konsequenz aus dem Ziel, dass der Einzelne vor einer Beeinträchtigung seines Rechtes geschützt werden soll, „aus eigener Entscheidung zu planen und zu agieren“. Voraussetzung dafür ist es wenigstens einigermaßen abschätzen zu können, welche ihn betreffenden Informationen in seinem sozialen Umfeld bekannt sind. Diese Selbstbestimmungsmöglichkeit setzt also Kenntnis voraus, weshalb alle Datenverarbeitungsprozesse so transparent wie möglich sein müssen. Dies bedeutet jedoch nicht, dass die verarbeiteten Daten für Jedermann transparent sein sollen, sondern nur die Bedingungen, unter denen die Daten verarbeitet werden.

Eine entsprechende Satzungsregelung für das Live-Streaming könnte wie folgt ausgestaltet sein:

- E(4) Der Umstand der Aufzeichnung und die verantwortliche Stelle sind mit der Einladung mitzuteilen und vor Betreten des Sitzungsraumes kenntlich zu machen. Zu Beginn der Sitzung weist der Sitzungsleiter die Teilnehmer auf ihr Widerspruchsrecht hin, das gegenüber dem Sitzungsleiter auszuüben ist.

## Einwilligung

Eine Einwilligung kann nur im Rahmen der gesetzlichen Grenzen des DSG MV die fehlende gesetzliche Grundlage ersetzen. Hier bedarf die Einwilligung „der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. … Der Betroffene ist in geeigneter Weise über die Bedeutung und Tragweite der Einwilligung, insbesondere über die Art und den Umfang der Verarbeitung sowie über Empfänger beabsichtigter Übermittlungen von Daten, aufzuklären. … Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.“

Eine Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dies kann also nur der Fall sein, wenn der Betroffene, in Kenntnis aller Umstände (auch der rechtlichen und tatsächlichen Folgen seine Einwilligung) frei von sachfremden Erwägungen („Haben Sie etwa was zu verbergen?“) ohne Nachteile befürchten zu müssen, entscheiden kann.

Im Unterschied zur gesetzlichen erlaubten Live-Übertragung durch die Medien oder durch eine Erlaubnis nach

der Hauptsatzung der Gemeinde braucht es ohne eine solche Satzungsregelung die individuelle Einwilligung. Dann würde also ein einzelner Widerspruch ausreichen, um ein Verbot der Verbreitung von Bildern und Ton von dieser Person zu rechtfertigen.

Auch aus Praktikabilitätsgründen wird die Einwilligung aller potentiell betroffenen Sitzungsteilnehmer (Wahlbeamte, Gemeindevertreter, Verwaltungsmitarbeiter, sachkundige Bürger, Zuschauer) selten rechtswirksam einzuholen sein. Deshalb kann nur eine Satzungsregelung die nötige Rechtsgrundlage für Live-Streaming schaffen.

## Anforderungen an die behördliche Organisation

### Frühzeitige Einbeziehung des behördlichen Datenschutzbeauftragten

Jede Behörde hat einen Datenschutzbeauftragten und einen Vertreter schriftlich zu bestellen und diesem die erforderliche sachliche und finanzielle Ausstattung zur Erfüllung seiner Aufgabe als interner, aber unabhängiger Kontrolleur zu gewähren. Der behördliche Datenschutzbeauftragte hat neben der Überwachung aber vor allem die Aufgabe, die Mitarbeiterinnen und Mitarbeiter bei der Anwendung des Datenschutzrechtes zu beraten und auf die Einhaltung der Vorschriften „hinzuwirken". Auch ohne gesetzliche Verpflichtung hat er selbstständig und unabhängig jedes neue Datenverarbeitungssystem, den geplanten Einsatz von Videoüberwachung oder auch die Beschaffung neuer Kommunikationstechnik auf die Einhaltung der datenschutzrechtlichen Anforderungen hin zu untersuchen und dieses Ergebnis gegenüber der Behördenleitung zu vertreten. Dies gilt erst Recht bei einem Projekt wie der Einführung eines Live-Streamings.

Der Datenschutzbeauftragte der Behörde ist aber auch Ansprechpartner der Bürgerinnen und Bürger bei Fragen oder Beschwerden über den Umgang der Behörde mit seinen Daten. Deshalb sollte auch eine Kontaktmöglichkeit beispielsweise im Internetangebot offen kommuniziert werden. Zumindest alle Mitarbeiterinnen und Mitarbeiter müssen wissen, wer in ihrer Behörde der Ansprechpartner für Fragen und Probleme ist.

Mit seiner Funktion als unabhängige Kontrollstelle ist der Datenschutzbeauftragte der natürliche Verbündete der Kommunalvertretung, wacht er doch – wie auch die Abgeordneten – über den rechtmäßigen Umgang der Verwaltung mit Bürgerdaten. Aber auch die Abgeordneten können sich in ihrer Tätigkeit beim behördlichen Datenschutzbeauftragten Rat holen.

Im Rahmen von Gemeindevertretungssitzungen wirken auch Mitarbeiterinnen und Mitarbeiter der Gemeinde mit, ohne gewählt zu sein. Entweder als Unterstützungskräfte für die Versammlungsleitung oder als sachkundige Auskunftspersonen können sie somit auch im Rahmen eines Live-Streamings betroffen sein. Damit ist der Personalrat in die Vorbereitung einzubeziehen, da diesem eine eigenständige Verantwortung bei der Verarbeitung personenbezogener Daten der Mitarbeiter zukommt, §§ 61 Nr. 2, 70 Abs. 1 Nr. 1 PersVG.

### Technisch-organisatorische Maßnahmen

Das Gesetz verlangt von allen Behörden und öffentlichen Stellen die Sicherstellung der technischen und organisatorischen Maßnahmen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind. Deshalb ist es im Datenschutzgesetz von Mecklenburg-Vorpommern zwingend vorgeschrieben (§ 22 Abs. 5 DSG MV), für Systeme der automatisierten Datenverarbeitung ein Sicherheitskonzept zu erstellen. In diesem Sicherheitskonzept sind sowohl die Schutzbedarfsfeststellung als auch die getroffenen Sicherheitsmaßnahmen zu dokumentieren und regelmäßig fortzuschreiben.

Eine wirksame Maßnahme zur Eingrenzung der weltweiten Erreich- und Speicherbarkeit der übertragenden Videostreams ist die Eingrenzung der IP-Adressräume für den Empfang der Übertragung bzw. den Abruf der Daten. Dies wird zwar nicht überzeugend „gemeindescharf" möglich sein, aber zumindest der Zugriff von Servern aus anderen Ländern kann so eingegrenzt werden.

### Verfahrensverzeichnis

Das wichtigste Planungs- und Organisationsmittel ist das Verfahrensverzeichnis, das für jede öffentliche Stelle die Beschreibungen der verwendeten Datenverarbeitungssysteme enthält und – mit Ausnahme der sicherheitsrelevanten Angaben – jedermann zur Einsicht gegeben werden muss. Damit kann jeder Bürger ohne eine Begründung erfahren, wie die Verwaltung mit seinen Daten umgeht. Hier ist auch das Live-Streaming als ein Verfahren aufzunehmen.

Inhalt Verfahrensbeschreibung: die Bezeichnung des Verfahrens und der verarbeitenden Stelle, den Zweck und die Rechtsgrundlage der Verarbeitung, die Art der gespeicherten Daten, den Kreis der Betroffenen, den Kreis der Empfänger, denen die Daten mitgeteilt werden, geplante Datenübermittlungen in Drittländer, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 21 und 22.

Das Verfahrensverzeichnis führt der behördliche Datenschutzbeauftragte, der dieses auch zur Einsichtnahme bereithalten muss. Dem Transparenzgrundsatz folgend bietet es sich jedoch an, dieses Verfahrensverzeichnis auf der Internetpräsentation der öffentlichen Stelle zu veröffentlichen.

### Auftragsdatenverarbeitung

Besondere Pflichten ergeben sich aus der Beauftragung eines Dienstleisters. Hierzu hat der LfD MV eine Orientierungshilfeherausgegeben.[14] § 4 DSG MV legt die bei einer Auftragsdatenverarbeitung zu beachtenden Anforderungen fest und stellt in Absatz 4 ausdrücklich klar, dass auch bei Wartungs- und Fernwartungsarbeiten sowie bei anderen Hilfstätigkeiten die Vorschriften über Auftragsdatenverarbeitung entsprechend anzuwenden sind, so beispielsweise, wenn private Dienstleister Software installieren, pflegen oder korrigieren oder Hardware überprüfen, reparieren oder austauschen.

Das Übertragen und Aufzeichnen von Sitzungen der Gemeindevertretung

stellt eine Datenverarbeitung dar, für die im Fall der Beauftragung durch die Gemeinde ein Vertrag erforderlich ist.

Der Auftrag zur Verarbeitung personenbezogener Daten ist schriftlich zu erteilen. Die wesentlichen Aspekte, wie Art und Umfang der Verarbeitung sowie die technischen und organisatorischen Maßnahmen, sind detailliert und verbindlich festzulegen. Der nachfolgende Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag soll als Orientierungshilfe bei der Auftragsvergabe dienen und ist im Einzelfall aufgabenspezifisch anzupassen. Durch die Auftragsgestaltung muss gewährleistet sein, dass das für öffentliche Stellen geltende Datenschutzrecht in vollem Umfang berücksichtigt und das hohe Datenschutzniveau beibehalten wird. Voraussetzung hierfür ist unter anderem, dass der Auftragnehmer unter besonderer Berücksichtigung seiner Eignung ausgewählt wird. Der Auftraggeber hat dabei zu prüfen, ob der Auftragnehmer die erforderlichen Sicherheitsmaßnahmen nach §§ 21 und 22 DSG MV realisieren kann. Gemäß § 4 Abs. 3 Satz 2 DSG MV ist der Auftraggeber verpflichtet, den Landesbeauftragten für den Datenschutz über die Beauftragung von Stellen zu unterrichten, die nicht unter das DSG MV fallen.

1 http://www.datenschutz-mv.de/informationsfreiheit/themen/themen_eval.html.

2 Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 / Volkszählungsurteil – 1 BvR 209/83 u.a., in Auszügen als Anhang 3 in: BfDI-INFO 1 Bundesdatenschutzgesetz - Text und Erläuterung -, Bundesbeauftragter für Datenschutz und Informationsfreiheit (Hrsg.), kann kostenlos bezogen werden unter: http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Infomaterial/BfDInformationsbroschueren/BfDInformationsbroschueren_node.html

3 Vgl. Internetveröffentlichung über Empfänger von Agrarzuwendungen aus EU-Mitteln, Oberverwaltungsgericht für das Land Mecklenburg-Vorpommern 2. Senat, Beschluss vom 04.05.2009, 2 M 77/09.

4 Zum Problem der Informationen, die als Suchbegriffe im Google-Cache nach der Löschung der Seite automatisch über Monate gespeichert bleiben können vgl. 5.4.5 im Zehnten Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), Landtag MV, Drs. 6/712 vom 02.05.2012, S. 105 f..

5 Zu den Unterschieden zwischen Parlament und Vertretung und sich daraus ergebenen Differenzierungen siehe ausführlich: „Live-Übertragung der Sitzungen der Bezirksverordnetenversammlung (BVV) via Internet“ in: Berliner Beauftragter für Datenschutz und Informationsfreiheit (Hrsg.), Dokumente zu Datenschutz und Informationsfreiheit 2011, S. 140 ff., http://www.datenschutz-berlin.de/content/veroeffentlichungen/dokumente/dokumente-2011.

6 BVerfG, Urteil vom 24.01.2001 – 1 BvR 2623/95, 1 BvR 622/99 – zur Medienöffentlichkeit in Gerichtsverhandlungen.

7 Gesetzentwurf der Landesregierung, Entwurf eines Gesetzes über die Kommunalverfassung und zur Änderung weiterer kommunalrechtlicher Vorschriften, Landtag MV, Drs 5/4173, S. 133.

8 OVG des Saarlandes, 3, Senat, Beschluss vom 30.08.2010, Az: 3 B 203/10, zitiert nach Juris, zu einem Antrag einer privaten Rundfunkveranstalterin, die öffentlichen Sitzungen eines Stadt- oder Gemeinderates in Ton und Bild zum Zwecke der Rundfunkberichterstattung aufzeichnen zu dürfen, Rn 17, mit weiteren Nachweisen.

9 Siehe zum Problem von Handy-Fotos im Netz 5.7.2 im Zehnten Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), Landtag MV, Drs. 6/712 vom 02.05.2012, S. 109 f.

10 Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (Hrsg.), Landesdatenschutzgesetz mit Erläuterungen, Schwerin 2011, zu § 7, S. 56.

11 Ebenda, zu § 7, S. 56.

12 andere Auffassung Wacker/Supper: Liveübertragung von Ratssitzungen im Internet in: RDV 2013, 147 ff.; allerdings unter unzutreffender Bezugnahme auf Landesdatenschutzbeauftragter Bayern, 21. Tätigkeitsbericht, Pkt. 11.2 (mit deutlichen Hinweisen auf Möglichkeiten gesetzgeberischer Regelungen) und ebenso unzutreffend auf BVerwG Urt. v. 03.08.1990 – 7 C 14/90 – hier ging es um Tonaufnahmen eines Journalisten gegen den Beschluss der Vertretung unter Betonung, dass das Persönlichkeitsrecht der einzelnen Ratsmitglieder hier nicht einer solchen entgegenstehen würde, sondern allein die durch Beschluss der Gemeindevertretung als gefährdet definierte Funktionsfähigkeit des Parlamentes (Rn 14);

für eine Satzungsregelung: VG Kassel 3. Kammer, Beschluss vom 07.02.2012 – 3 L 109/12.KS, zur Rechtslage in Hessen;

in der Abwägung mit der Pressefreiheit das datenschutzrechtliche Widerspruchsrecht eines einzelnen Kommunalvertreters ebenfalls ablehnend: OVG des Saarlandes 3. Senat, Beschluss vom 30.08.2010 – 3 B 203/10

13 BVerwG, Beschluss vom 26.03.1985, Az.: 6P31/82

14 Quelle: http://www.lfd.m-v.de/datenschutz/publikationen/muster.html ; Bearbeitung durch den Autor.

Thilo Weichert

# Prism, Tempora, Snowden … Analysen und Perspektiven

## I. Wir konnten es ahnen

Niemand hätte überrascht sein müssen: Die Mosaiksteine der Bilder der US-amerikanischen und der britischen Telekommunikations- und Internetüberwachung, die mit den Begriffen „Prism“[1] und „Tempora“[2] bekannt wurden und sich mit den Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden immer weiter präzisierten, sind lange bekannt: Dass die National Security Agency (NSA) für die US-Sicherheitsbehörden weltweit die irgendwie erreichbaren Daten erfassen, weitergeben und analysieren[3] ebenso wie für Großbritannien das Government Communication Headquarters (GCHQ)[4], war in Medien nachzulesen. Die Rechtsgrundlagen für deren Spitzelaktionen, insbesondere der Patriot Act und der Foreign Intelligence Surveillance Act (FISA) für die USA[5] sowie der Regulation of Investigatory Powers Act (RIPA) für Großbritannien[6], waren bei ihrer Verabschiedung und den späteren Verschärfungen und Verlängerungen jeweils heiß umstritten. Dass NSA und GCHQ riesige Personalapparate und gewaltige Rechenzentren zur Verfügung haben, haben investigative Journalisten auch schon vor längerer Zeit herausgefunden.[7] Das reduzierte Datenschutzverständnis unserer angloamerikanischen und angelsächsischen Freunde westlich und östlich des Atlantiks verursacht uns Datenschützern schon seit Jahren große Bauchschmerzen.[8] Was mit moderner Speichertechnik und Big-Data-Analysen möglich ist, wird uns täglich von der informationstechnischen (IT-) Industrie in Hochglanz angepriesen.[9] Dass tatsächlich gemacht wird, was technisch an Datenspeicherung und -auswertung möglich ist und nützlich erscheint, fürs Geldverdienen oder für die Sicherheit, wenn niemand Unabhängiges kontrolliert, das wissen zumindest erfahrene Datenschützer seit mehr als drei Jahrzehnten.

Unsere Befürchtung, dass von US-amerikanischen und britischen Sicherheitsdiensten eine gewaltige Gefahr für das ausgeht, was das deutsche Bundesverfassungsgericht im Jahr 1983 „Recht auf informationelle Selbstbestimmung“ genannt und begründet hat,[10] wird nun durch immer mehr Details zur Gewissheit. Diese Rechtsprechung ist seit 2009 in Art. 8 der Europäischen Grundrechtecharte als „Grundrecht auf Datenschutz“ europaweit geltendes Verfassungsrecht und individualrechtlicher Anspruch. Wir müssen dem Edward Snowden unendlich dankbar sein, dass er unsere Unsicherheit beseitigt hat, indem er unsere Befürchtungen bestätigte: Wir wissen seit seinen ersten Enthüllungen, dass die USA und Großbritannien von Hunderten Millionen, ja wohl Milliarden unverdächtigen Menschen sensible Telekommunikations- und Internetdaten auswerten – mit der Begründung, den Terrorismus zu bekämpfen.

## II. Nicht Datenschutz contra Sicherheit

Wir wissen, dass die Bekämpfung des Terrorismus oder sonstiger gemeinschädlicher Verbrechen ohne Missachtung unserer Grundrechte möglich ist. Wir wissen, dass eine derartige Grundrechtsmissachtung letztlich in die Hände der Terroristen und Verbrecher spielt: Das deutsche Bundesverfassungsgericht hat entgegen den Empfehlungen von „Sicherheitsexperten“ dem deutschen Gesetzgeber immer wieder die rote Karte gezeigt, nachdem dieser den Sicherheitsbehörden weitergehende, manchmal uferlose Befugnisse zuschanzen wollte: großer Lauschangriff, Telekommunikationsüberwachung, KFZ-Kennzeichenerkennung, Rasterfahndung, BKA-Gesetz, Vorratsdatenspeicherung, Antiterrordateigesetz… die Liste der geduldigen, jeweils gut begründeten Urteile und Ermahnungen, im Namen der Sicherheit die Freiheit nicht über Bord zu werfen, ist lang. Für manche mag erstaunlich sein, dass trotz der Einhegung und Disziplinierung unserer Sicherheitsbehörden die Kriminalität und der Terrorismus in Deutschland erheblich geringer sind als etwa in den USA oder in Großbritannien.

Was für einfache Gemüter erstaunlich sein mag, ist bei nüchterner Betrachtung logisch: Vertrauen ist eine bessere Sicherheitsgrundlage als Angst und Kontrolle. Die Überwachung der gesamten Bevölkerung für Sicherheitszwecke ist unsinnig, weil die meisten Menschen sich im großen Ganzen ehrbar und rechtstreu verhalten. Menschen mit Überwachung zu überziehen, lässt sie an der Ernsthaftigkeit der gesellschaftlichen, politischen und rechtlichen Freiheitsverbürgungen zweifeln und veranlasst sie, dort ihren Vorteil zu suchen, wo die Überwachung nicht ganz so groß erscheint.

Verhältnismäßiges Vorgehen ist insbesondere im Hinblick auf unsere gesellschaftlichen Minderheiten geboten, seien es Muslime, Angehörige arabischer Staaten, Schwule, politisch Andersdenkende oder Menschen mit anderer Hautfarbe oder ungewohntem Aussehen: Als ungerecht empfundene Kontrollen und Überwachung und damit verbundene Ausgrenzung sind der Nährboden für Angst und Aggression bei den Betroffenen. Und dies ist eine wesentliche Grundlage für Hass und Gewaltbereitschaft, bis hin zu terroristischem Fanatismus. Etwas technischer Sachverstand müsste „Sicherheitsexperten“ bewusst ma-

chen, dass unkontrollierte Kontrollen und insbesondere die Totalkontrolle der Bevölkerung kontraproduktiv sind: Da diese Kontrollen nie völlig perfekt sein können und technische Schutzmaßnahmen eher von den professionellen Kriminellen als den arglosen Bürgern praktiziert werden, geraten außer den Unschuldigen allenfalls kriminelle Amateure bei Rasterfahndungen ins Netz. Den Profis kommen wir nur auf die Schliche, indem wir verdachtsbezogen konkreten Hinweisen gezielt nachgehen.[11]

Das vom deutschen Bundesverfassungsgericht geforderte freiheitliche Verständnis von Sicherheit steht in diametralem Widerspruch zum Sicherheitsdenken in Diktaturen oder Überwachungsstaaten wie z. B. China. Es steht aber auch in Widerspruch zur gelebten Sicherheitspolitik der USA, die sich in ihrer Logik nur wenig von der Russlands oder Chinas unterscheidet. Die US-Realität ist auch möglich, weil es in den USA kein Grundrecht auf Datenschutz, also ein Grundrecht gegen Überwachung, gibt. Von den vom US-Supreme Court eingeforderten „reasonable expectations of privacy" sind bisher Sicherheitsbehörden und Internetfirmen weitgehend ausgenommen.[12]

## III. US-Kooperation contra Datenschutz

Dies hat Europa ignoriert, als es Kooperationsabkommen mit den USA abschloss, z. B. über die Weitergabe von Fluggast- oder Banktransaktions- oder sonstigen Daten an Sicherheitsbehörden, aber auch mit der Zulassung des transatlantischen Datentransfers zwischen Firmen durch Selbstzertifizierung gemäß den Safe-Harbor-Principles. Dass die „vernünftigen Erwartungen an Privatheit" auch faktisch derart verletzt werden, wissen wir erst seit wenigen Tagen mit Gewissheit. Dadurch ist die Geschäftsgrundlage für die Abkommen zum Datenaustausch weggefallen. Deshalb müssen diese Abkommen hinterfragt und im Zweifel gekündigt werden. Der CDU-Europaparlamentarier Elmar Brok meinte: „Europäer müssen in den USA denselben Rechtsschutz bekommen wie amerikanische Staatsbürger. Diese Forderung ist mit uns nicht verhandelbar".[13] Die Konferenz der deutschen Datenschutzbeauftragten des Bundes und der Länder wies darauf hin, dass die von der EU-Kommission festgelegten Grundsätze des „sicheren Hafens" (Safe Harbor) zum Datentransfer in die USA (2000) und zu Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) nur gelten können, wenn die Empfänger einem angemessenen Datenschutzniveau unterliegen. Ein Aussetzen der Datenübermittlungen sei möglich, wenn eine „hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind. Dies sei nun der Fall.[14] Damit setzten sie sich von ihrem irischen Kollegen ab, der auch nach Bekanntwerden der NSA-Zugriffe auf Daten von Facebook und Apple keinen Anlass zum Tätigwerden sah und sieht.[15]

Neue Abkommen, etwa über eine transatlantische Freihandelszone, sind ohne die Gewährleistung von Datenschutz in den USA angesichts der expandierenden Informationswirtschaft nicht denkbar. Wenn europäische Politiker meinen, sich ökonomisch den Wanst füllen zu können, ohne sich dabei zugleich mit der US-amerikanische Krankheit der Datenschutzverweigerung zu infizieren, betreiben sie Selbst- und Fremdbetrug.

Die Datenschutzignoranz von US-Regierung und US-Industrie verfolgt zwei Ziele: die Erhaltung der globalen sicherheitspolitischen Dominanz und die Bewahrung der Dominanz von US-Informationstechnikunternehmen auf dem Weltmarkt. Diese Ignoranz bzw. dieses Verleugnen wird in den USA leider im Einverständnis von Republikanern und Mehrheitsdemokraten gegen eine aktive Bürgerrechtsopposition durchgesetzt. In dieser Opposition hat Europa mit seinem Grundrechtsverständnis viele natürliche Verbündete. Doch diese Bürgerrechtsopposition hat einen ungemein schwereren Job als die Datenschützer in Europa: Seit über 50 Jahren kämpfen sie für „Privacy and Freedom" - bisher ohne nachhaltigen Erfolg.[16]

## IV. Edward Snowden

Die Doppelmoral des Vorgangs um Prism und Tempora zeigt sich am offensichtlichsten am Umgang mit Edward Snowden. Es ist eine Bankrotterklärung der westlichen Gesellschaften, die sich demokratisch und freiheitlich bezeichnen, dass Snowden erst in China und dann in Russland Schutz suchen muss und findet. Es ist erschreckend, mit welcher Vehemenz die US-Regierung auf alle Staaten Druck ausübt, die in Frage kommen, Asyl zu gewähren, um eines „Verräters" habhaft zu werden, nicht eines Menschen mit dem Ziel der Verwirklichung von Freiheitsrechte und demokratischer Transparenz. Snowden achtete sorgsam und bisher erfolgreich darauf, dass durch seine Offenlegung keine Menschen Schaden erleiden. Derweil veranlassen die USA die Zwischenlandung und Durchsuchung des Flugzeugs des bolivianischen Präsidenten Evo Morales in Wien gemäß dem erklärten Motto: „Wir jagen Snowden bis ans Ende der Welt und führen ihn seiner Bestrafung zu".[17] Diese Verfolgung ist politische Verfolgung, für die gemäß Art. 16a Abs. 1 GG in Deutschland Schutz gewährt werden muss. Die Bundesregierung ignoriert auch dieses Grundrecht und verweigert die Einreise. Damit begibt sie sich der großen Chance, weitere Informationen zu erlangen, mit denen die USA zu einem Einlenken in Sachen Datenschutz veranlasst werden kann. Während Deutschland die Chance verspielt, mit einer Aufnahme Snowdens, die von ihm erbeten wurde, ein klares Zeichen zu setzen, ist dieser dem politischen Kalkül von Staaten ausgeliefert, deren Gesellschaftsordnung nicht mit seinen – vom europäischen Verfassungsrecht geschützten – Beweggründen und Werten in Einklang stehen.[18] Die freiheitliche Bankrotterklärung erfolgte, als US-Justizminister Eric Holder am 26.07.2013 erklärte, Snowden müsse in den USA keine Todesstrafe und keine Folter befürchten.[19]

## V. Der Beginn einer langen Auseinandersetzung

Was ist zu tun? Zweifellos müssen die Sachverhalte weiter aufgeklärt werden, und zwar nicht hinter verschlossenen Türen, sondern öffentlich. Hierin kann und darf aber nicht der Schwerpunkt liegen. Das Infragestellen und im Zweifel das

Aufkündigen von grundrechtlich nicht akzeptablen Datenaustauschabkommen muss der nächste Schritt sein. Zur rechtlichen Aufarbeitung gehört auch, die straf-, zivil- und vor allem die freiheitsrechtliche Verantwortlichkeit von handelnden Personen und Institutionen zu untersuchen. Sollte die europäische Justiz der „Täter" mit Sitz in den USA nicht so leicht habhaft werden, die britischen Verantwortlichen für die Aktivitäten des GCHQ unterliegen europäischem Recht, das durch die nationalen Regierungen, das Europäische Parlament, den Rat und die Kommission der EU eingefordert werden muss und vor dem Europäischen Gerichtshof in Luxemburg sowie dem Europäischen Menschenrechtsgerichtshof in Straßburg durchgesetzt werden kann.

Die selbstverständlichste Reaktion Europas sollte es sein, die US-amerikanischen Datensauger à la Google, Facebook, Apple, Amazon u. a. zumindest soweit zur Beachtung des europäischen Rechts zu zwingen, wie diese in Europa aktiv sind. Hierzu können die Verbraucherinnen und Verbraucher einen wichtigen Beitrag leisten. Sie sollten den Unternehmen klar machen, dass sie sich zwischen zwei Alternativen entscheiden können: die informationelle Ausbeutung und Fremdbestimmung der europäischen Verbraucherinnen und Verbraucher beenden und den Datenschutz zu beachten – oder vom Markt zu verschwinden.

Selbstdatenschutz ist wichtiger denn je. Grundprinzipien sind hierbei Datenvermeidung und Datensparsamkeit, also so wenige Daten im Netz zu hinterlassen wie irgend möglich: Nutzung datensparsamer Internetangebote ohne Datenspuren zu hinterlassen, bei Suchmaschinen z. B. des als datenschutzkonform zertifizierten Ixquick/Startpage. Beim Surfen können Anonymisierungsdienste verwendet werden. Das deutsche Telemediengesetz erlaubt ausdrücklich – entgegen der Praxis von US-Firmen – Pseudonyme statt Klarnamen. Durch Verwendung mehrerer Browser, mehrerer E-Mail-Accounts oder mehrerer sonstiger Identitäten wird eine Profilbildung erschwert. Bei der Datenspeicherung – jedenfalls in der Cloud – und bei sensiblen E-Mails sollten die Daten verschlüsselt werden. Tracking-Blocker und das Löschen von Cookies im Browser erschweren das Tracking. Wenn es bei den Browsereinstellungen schon kein „Privacy by Default" gibt, dann sollten diese gemäß den individuellen Datenschutzwünschen verändert werden.

Bei der Auswahl von Internetdiensten sind europäische und deutsche Angebote den Angeboten aus Drittländern, insbesondere aus den USA, vorzuziehen, weil dann sicher europäisches Datenschutzrecht anwendbar ist. Auch bzgl. britischer Anbieter ist größere Vorsicht und Zurückhaltung geboten. Datenschutzbewusstes Verbraucherverhalten im Internet wird von den Betreibern registriert und eröffnet die Chance, dass sich über den Wettbewerb datenschutzkonforme Produkte durchsetzen.[20]

Der Kampf um eine demokratische und freiheitliche Informationsgesellschaft ist noch lange nicht verloren. Dieser Kampf hat gerade erst begonnen. Bei diesem globalen Kampf stehen uns moderne autoritäre Staaten wie Russland und China gegenüber. Die USA müssen sich entscheiden, auf welcher Seite sie stehen. Wir sollten uns darauf einstellen, eine lange Auseinandersetzung zu führen.

1 Tagespresse seit dem 06.06.2013; NSA collecting phone records of millions of Verizon customers daily, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Sokolow, http://www.heise.de/newsticker/meldung/Big-Data-fuer-Big-Brother-Liest-der-US-Geheimdienst-immer-mit-1884735.html?view=print,.

2 Tagespresse seit 21.06.2013, Askill/Borger/Hopkins/Davies/Ball, http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet.

3 Inhaltsaufzeichnung von digitaler Kommunikation, DANA 2/2013, 72; US-Studien warnen vor behördlicher US-Überwachung bei Cloud-Diensten, DANA 1/2013, 26; Millionen Mobilkommunikationsdaten für Ermittlungsbehörden, DANA 3/2012, 128; Schwere Rechtsbrüche des FBI beim Anti-Terror-Kampf, DANA 1/2011, 26; Regierung zu Schadenersatz wegen NSA-Abhörprogramm verurteilt, DANA 1/2011, 29.

4 Regierung plant massive Ausweitung der Verkehrsdatenüberwachung, DANA 2/2012, 90; Teure Abhörzentrale nimmt Arbeit auf, DANA 4/2003, 28.

5 Neue Gesetze zur Internetkontrolle, DANA 1/2012, 32; Verlängerung von „Patriot Act" vorläufig gescheitert, DANA 1/2011, 27; FISA-Berufungsgericht erklärt Abhören ohne Richterbeschluss für legal, DANA 1/2009, 33; Patriot Act bleibt kurzfristig weiter bestehen, DANA 1/2006, 35 (2/2006, 91).

6 Rauhofer, Die Vorratsdatenspeicherung als Instrument sozialer Kontrolle – eine deutsch-britische Perspektive, DANA 2/2006, 58 f.; Überwachungsgesetz reißt Löcher in die Privatsphäre, DANA 2/2000, 32.

7 Poitras/Rosenbach/Schmid/Stark/Stock, Angriff aus Amerika, Der Spiegel 27/2013, 76 ff.

8 Weichert, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113 ff.; Korff, Guaranteeing Liberty or Big Brother – Surveillance in the United Kingdom, v. 24.08.2007; https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-korff-surveillance-in-the-united-kingdom-complete.pdf.

9 Weichert, Big Data und Datenschutz, ZD 2013, 251 ff.

10 BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

11 Weichert, Überwachung bringt nichts und macht aggressiv, 2006, https://www.datenschutzzentrum.de/polizei/weichert-ueberwachung2.htm.

12 Weichert, RDV 2012, 115 ff.

13 Europapolitiker Brok droht USA mit Aufkündigung wichtiger Abkommen, www.focus.de 27.07.2013.

14 Konferenz der Datenschutzbeauftragten, PE vom 24.07.2013, Geheimdienste gefährden den Datenverkehr zwischen Deutschland und außereuropäischen Staaten.

15 Irische Behörde: EU sah 2000 Prism voraus, www.europe-v-facebook.org 25.07.2013.

16 Westin, Privacy and Freedom, 1967, 487 S.

17 Hujer/Neef/Schepp, Finger in der Wunde, Der Spiegel 29/2013, 76 ff.

18 ULD: Schutz unserer Daten durch Schutz für Edward Snowden, PE 18.07.2013.

19 Keine Todesstrafe, SZ 27./28.07.2013, 5.

20 ULD: Prism/Tempora – Was wir dagegen tun können, PE 10.07.2013.

# NSA und Snowden...

## Geleitwort von Johannes Caspar zur Demonstration „Stop watching us“ am 27.7.2013 in Hamburg

Seit der Veröffentlichung der ersten Enthüllungen durch Edward Snowden Anfang Juni sind mittlerweile mehr als 7 Wochen vergangen. Was ist in dieser Zeit eigentlich geschehen?

Statt Aufklärung durch die verantwortlichen Stellen hat sich, was als Überwachungsskandal begann, zu einer Krise der demokratischen Rechts- und Verfassungsstaatlichkeit ausgeweitet. Verantwortliche Stellen in den USA bleiben angesichts der Enthüllungen sprachlos, aber auch die Bundesregierung sowie die Europäische Kommission, die sich schützend vor die digitalen Grundrechte der Bürger stellen sollten, haben bisher zur Aufklärung der Vorwürfe nicht beigetragen. Stattdessen werden immer neue Verstrickungen in das System flächendeckender Überwachung bekannt. Der britische Geheimdienst nimmt unter dem Codewort Tempora eine massive flächendeckende Überwachung der Telekommunikation und des Internetdatenverkehrs in Europa vor. Mittlerweile erreichen die Meldungen über die Ausspähungen auch das Bundeskanzleramt: Die deutschen Geheimdienste BND und Verfassungsschutz setzen offenbar die Software XKeyScore ein. Ein Instrument der NSA, mit dem immerhin 180 Millionen der 500 Millionen Datensätze, die allein im Dezember 2012 gespeichert wurden, erfasst worden sein sollen. Man möchte gar nicht wissen, was noch alles an das Tageslicht drängt.

In diesem Sommer muss man Angst haben um die Privatsphäre der freien Welt. Die digitalen Techniken haben uns angreifbarer gemacht. Die Schutzhülle der Grundrechte erweist sich gegenüber der massiven Ausspähung durch Geheimdienste als unerwartet verletzlich. Rechts- und Verfassungsstaatlichkeit sind in massiver Weise in Frage gestellt. Die Versuche, sie wieder herzustellen, waren bislang eher halbherzig und resignativ. Sie haben nicht einmal die Klärung gebracht, die unabdingbar ist, um das systematische Ausspionieren in seiner ganzen Dimension zu begreifen. Fast ist es, als habe uns dieser Sommer brutal vor Augen geführt, dass wir lange mit einer Illusion lebten: der Illusion, dass die Freiheit der digitalen Welt sich in freien Gesellschaften nicht gegen die Freiheit selbst kehren kann.

Die demokratischen Verfassungsstaaten stehen derzeit vor einer Herausforderung historischer Dimension. Wir befinden uns in einer Vertrauenskrise des auf die Geltung von Grundrechten angelegten Rechts- und Verfassungsstaats. Was wir gegenwärtig erleben ist nicht nur ein Skandal, der sich durch das gewöhnliche Instrumentarium parlamentarischer Untersuchungsausschüsse, öffentlicher Diskurse und möglicherweise der Anrufung des Bundesverfassungsgerichts hinlänglich aufarbeiten ließe. Qualitativ wie auch quantitativ erweisen sich die Anstrengungen staatlicher Stellen, die Datenwelt des Einzelnen vollständig zu überwachen, als ein unmittelbarer Angriff auf das Rückgrat des Systems der Grundrechte. Das Besondere daran: Es handelt sich um einen Angriff von innen. Geführt wird er in einer Haltung, die die Sicherheit über die Werte der Freiheit und Transparenz offener Gesellschaften stellt und die sich als Verfassungsziel selbst legitimiert. Derzeit ist nicht abzusehen, welchen Ausgang das Ringen um die digitalen Grundrechte haben wird. Klar ist: Sicherheit ohne Freiheit ist das Ende des Entwurfs des demokratischen Verfassungsstaats.

Sieben Wochen nach der ersten Enthüllung bleibt auch die Erkenntnis: Dass wir uns an all das gewöhnen, darf niemals eintreten! Wir werden sonst Schritt für Schritt zu digitalen Untertanen, die sich im Namen der Sicherheit anlasslos ausforschen lassen, denn sie haben ja nichts zu verbergen. Am Ende aber steht ein kollektiver Verlust der Freiheit. Wenn das staatliche System der Ausforschung unseres Privatlebens keine weitergehenden negativen Konsequenzen für die meisten von uns nach sich zieht und wenn die anlasslose Speicherung der Daten der Bürger am Ende nicht das filigrane Gefüge demokratischer Rechtsstaatlichkeit kollabieren lässt, dann haben wir nur Glück gehabt.

Es ist an uns allen, eine freiheitliche Welt der Kommunikation und Information bei der Politik einzufordern. Es gilt daher für jeden, sich dafür einzusetzen, dass das, was jetzt im Sommer 2013 wie ein böser Traum erscheinen mag, nicht als eine Realität zu akzeptieren, in der wir künftig leben wollen.

## Pressemitteilung vom 14. August 2013

# Erste weltweit koordinierte Zusammenarbeit der Aufsichtsbehörden bringt erhebliche Defizite im Datenschutz ans Licht

Zum ersten Mal haben in diesem Jahr neunzehn Datenschutzaufsichtsbehörden aus aller Welt im Rahmen des „Global Privacy Enforcement Networks" (GPEN) zusammengearbeitet und in ihren jeweiligen Ländern untersucht, ob Unternehmen und Daten verarbeitende Stellen bei Internetseiten und mobilen Applikationen ein transparentes Verhalten gegenüber ihren Kunden zeigen. Den Anstoß dazu gab eine Initiative der Datenschutzbehörde Kanadas.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, erklärt hierzu: „Es ist das erste Mal, dass sich im Rahmen dieser gemeinsamen Aktion fast zwanzig Datenschutzbehörden zusammen gefunden haben, um weltweit die Transparenz und Offenheit der Datenverarbeitung zu untersuchen. Die Prüfungen, die meine Mitarbeiter bei E-Mail- und Postdiensten durchgeführt haben, haben im Ergebnis gezeigt, dass sie die datenschutzrechtlichen Vorgaben ernst nehmen und entsprechend umsetzen."

Insgesamt wurden weltweit mehr als 2.200 Internet-Seiten und mobile Applikationen untersucht. Die Auswertung der weltweiten Ergebnisse hat erbracht, dass hiervon 23 % überhaupt keine Information zur Verarbeitung personenbezogener Daten ihrer Kunden bereitstellen. Insgesamt fanden die Aufsichtsbehörden bei rund 50 % aller untersuchten Internet-Seiten einen oder mehrere Mängel bezüglich Relevanz und Verständlichkeit der Information oder im Hinblick auf die Erreichbarkeit der verantwortlichen Stelle (Kontaktdaten) für mögliche Nachfragen oder Beschwerden durch deren Nutzer. Frappierend war allerdings, dass die Mängelrate bei mobilen Applikationen mit 90 % erheblich höher lag als bei Internet-Seiten.

Die genauen Ergebnisse der koordinierten Untersuchung der neunzehn Datenschutzbehörden sollen im Rahmen der 35. Internationalen Konferenz der Datenschutzbeauftragten vom 23.-26. September 2013 in Warschau vorgestellt werden. Unter den neunzehn beteiligten Behörden sind sechs aus Deutschland.

Für 2014 ist bereits eine weitere gemeinsame Aktion des GPEN zu einem anderen Aspekt des Datenschutzes geplant.

Pressestelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

Liebe Freunde und Abonnenten der Datenschutz Nachrichten

## Was wird sich im Jahr 2014 an der Arbeit der DVD und bei den Datenschutz Nachrichten ändern?

Hoffentlich werden die gegenwärtigen Datenschutz-Debatten die Aktualität und Dringlichkeit bürgerrechtlicher Standpunkte dermaßen unterstreichen, dass viele neue Mitstreiter unsere Stimme in der Öffentlichkeit noch stärker und hörbarer werden lassen. Bestimmt werden auch die Datenschutz Nachrichten weiter als fachlich und bürgerrechtlich orientierte Diskussions- und Informationsplattform über unseren Verein hinaus Bedeutung behalten. Bedauerlicherweise haben sich trotz ausschließlich ehrenamtlich arbeitender Redakteure und Autoren sowie vieler wirksamer Maßnahmen die Druck- und Versandkosten aber auch weiter entwickelt. Deshalb werden die Datenschutz Nachrichten ab dem Heft 1/2014 in gewohnter Qualität für 12 Euro zuzüglich Porto für ein Einzelheft, 42 Euro inklusive Porto für ein Abonnement im Inland und 52 Euro inklusive Porto für ein Auslands-Abo viermal im Jahr in Ihren bzw. Euren Briefkästen für fundierte und unabhängige Informationen sorgen.

# Datenschutznachrichten

## Datenschutznachrichten aus Deutschland

Bund

### Brief- und Paketdaten sind in Deutschland (begrenzt) geschützt

Als bekannt wurde, dass in den USA aus Sicherheitsgründen umfassend Metadaten von Postsendungen erfasst und gespeichert werden (s. u. S. 127), stellte sich die Frage, ob es eine derartige Praxis auch in Deutschland gibt. Tatsächlich scannt die Deutsche Post Angaben zu Briefen. Erfasst werden nach Postangaben nur die Adresse des Empfängers und die Freimachung. Diese Daten werden drei Tage lang gespeichert. Der Name des Empfängers sowie Angaben zum Absender würden nicht erfasst. Der aufgedruckte orangefarbene Barcode auf den Briefen enthält Angaben zur Empfangsadresse. Eine eindeutige Kennung bekommen normale Briefe im Gegensatz zu Einschreiben oder Paketsendungen aber nicht.

Mit Hilfe der drei Tage gespeicherten Daten könne man das Briefzentrum ermitteln, in dem die Adresse erfasst wurde, teilt die Post mit. In Deutschland seien das mehr als 80 Zentren, für den Großraum Hamburg gibt es zum Beispiel zwei solcher Einrichtungen. Damit Ermittler auf diese Daten zugreifen können, brauchen sie einen Gerichtsbeschluss. Das Postgeheimnis stellt in Deutschland offenbar eine Hürde für Ermittler dar, die Datensparsamkeit der Post dürfte außerdem dazu führen, dass die Daten nicht von all zu großem Interesse sind. Auch Verfassungsschutz, Militärgeheimdienst und Bundesnachrichtendienst können auf Daten zugreifen, wenn es um die Sicherheit der Bundesrepublik geht; Details regeln das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses sowie die Sicherheits- und Geheimdienstgesetze.

Bei Sendungen von Deutschland in die USA sieht es mit den Daten etwas anders aus: Zu Testzwecken werden die Daten von Paketsendungen von Geschäftskunden an die International Post Corporation (IPC) in Brüssel übermittelt. Davon erhoffen sich – gemäß Postangaben – die teilnehmenden Unternehmen aus derzeit 24 Industriestaaten eine Vereinfachung der Zollabfertigung. Auf diese Daten hat auch die US-Post Zugriff. An die Projektdatenbank der IPC werden, so die Post, rein warenbezogene Daten übermittelt, wie Gewicht und Warenbezeichnung, nicht jedoch personenbezogene Daten. Nach dem Grenzübertritt in die USA allerdings werden diese von der dortigen Post weitertransportiert – und vermutlich auch erfasst.

Express-Sendungen unterliegen besonderen Regeln. Sie werden nicht über das internationale Postsystem übertragen, sondern gelten als Frachtgüter. Die Sendungsdaten, Empfänger, Absender und Inhalt der Sendung, müssen der Grenzbehörde Customs and Border Protection seit 2004 vorab elektronisch übermittelt werden. Geregelt wird das über ein Handelsabkommen, die Öffentlichkeit erfuhr davon erst Jahre später (Reißmann, Deutsche Post erfasst nur Adressen, keine Namen, www.spiegel.de 08.07.2013).

Bund

### Studie zum Cybermobbing

Gemäß einer Studie „Cyberlife – Spannungsfeld zwischen Faszination und Gefahr“ des Bündnisses gegen Cybermobbing und der Versicherung ARAG sind ca. 17% der SchülerInnen in Deutschland schon Opfer von Cybermobbing geworden. 19% bekennen sich als TäterInnen. Die am 16.05.2013 in Köln vorgestellte Untersuchung erhebt keinen Anspruch auf Repräsentativität; sie ist aber die bislang umfassendste Studie zum Thema. Federführend bearbeitet wurde die Untersuchung von der Soziologin und Sozialpsychologin Catarina Katzer. Befragt wurden mehr als 10.000 Personen – SchülerInnen, Eltern und Lehrkräfte. Die Ergebnisse zeigen, wie verbreitet Mobbing im virtuellen Raum ist, und machen deutlich, wie hilflos Eltern und Lehrkräfte dem Problem gegenüberstehen. Zwischen 12 und 15 Jahren treten demnach die meisten Fälle von Cybermobbing auf. Mädchen werden häufiger Ziel virtueller Anfeindungen als Jungen.

Uwe Leest, Vorstandsvorsitzender des Bündnisses erläuterte. „Das Internet zieht immer mehr Störenfriede, Mobber, Sexualtäter und jene Personen an, die kriminelle Absichten hegen.“ Kinder seien besonders davon betroffen, da sie in einem multimedialen Zeitalter aufwachsen – ohne ausreichend darauf vorbereitet zu sein. Daher würden Forschung, Aufklärung und Präventionsarbeit „immer wichtiger, um das Phänomen Cybermobbing in den Griff zu bekommen“.

Die meisten Fälle treten an Berufsschulen, Hauptschulen (in Bayern Mittelschulen) und Realschulen auf. Gymnasien sind seltener betroffen. Über alle Schularten hinweg ist die Prävention von Cybermobbing mangelhaft, wobei mit Aufklärungsarbeit und einer Sensibilisierung wichtige Schritte geleistet werden können, um dem Problem entgegenzutreten. Der größte Teil der für Cybermobbing Verantwortlichen stammt aus dem sozialen Umfeld der Schule. Als Gründe werden vorrangig Langeweile und Spaß angegeben. Am häufigsten leiden SchülerInnen unter Beschimpfungen, Hänseleien und Lügen. Neben diesen „klassischen“ Formen des Mobbings machen sich die TäterInnen die Eigenschaften von sozi-

alen Netzwerken und Internetplattformen zunutze. So werden peinliche Bilder und Videos ohne Zustimmung veröffentlicht. Derartige Übergriffe haben eine besondere Wirkung, weil das „Cyberlife“ für junge Menschen eine immer größere Rolle spielt, so die Studie: „Die Täter kommen bis ins Kinderzimmer und die Opfer können sich kaum entziehen. Internet und Facebook sind überall“. Mehr als 80% der SchülerInnen haben einen eigenen Computer im Zimmer, 67% besitzen zudem ein internetfähiges Smartphone. Gegenüber traditionellem Mobbing an der Schule hat das Opfer keine Chance zu entkommen. Daher sei auch die Traumatisierung der Opfer bei dieser Form des Mobbings stärker: Mehr als ein Fünftel der Cybermobbing-Opfer fühlt sich durch die Attacken dauerhaft belastet. Eltern und Lehrkräfte bekommen die Nachstellungen im Netz häufig überhaupt nicht mit und fühlen sich nicht ausreichend über das Thema informiert. Nur 17% der Eltern überprüfen, was ihre Kinder im Internet machen. Lediglich 6% der befragten Eltern geben an, ihre Kinder regelmäßig beim Surfen im Netz zu begleiten. Diese mangelnde Kontrolle begründet knapp die Hälfte damit, sich zu wenig auszukennen. Und 57% der Eltern bestätigt, dass ihre Kinder mit dem Internet professioneller agieren als sie selbst. Fast 90% der Lehrkräfte berichtet, bereits Cybermobbingfälle unter ihren Schülern erlebt zu haben (Bruckner, Psychoterror im Netz, SZ 17.05.2013, 6; Stolzenbach, Tatort Facebook, /www.ksta.de 16.05.2013;). http://www.buendnis-gegen-cybermobbing.de/studie/cybermobbingstudie.pdf).

### Bund

## Visa-Warndatei in Betrieb

Das Bundesverwaltungsamt (BVA) hat Anfang Juni 2013 die Visa-Warndatei in Betrieb genommen: Sie soll die Visumbehörden bei ihrer Arbeit unterstützen und die Entscheidung über die Erteilung eines Visums auf eine breitere Grundlage stellen. Der Zugriff von Sicherheitsbehörden auf die Daten ist grundsätzlich nicht vorgesehen. Eine Ausnahme gilt für die mit der polizeilichen Kontrolle des grenzübergreifenden Verkehrs beauftragten Behörden für die Erteilung von Ausnahmevisa und Rücknahme von Visa an den Grenzen. In der Datei gespeichert werden Visumantragsteller, Einlader, Verpflichtungsgeber und sonstige Referenzpersonen, die mit Verurteilungen wegen bestimmter Straftaten mit Bezug zum Visumverfahren oder mit sonstigem Auslandsbezug oder mit konkreten sonstigen rechtswidrigen Verhaltensweisen wie insbesondere falschen Angaben im Visumverfahren aufgefallen sind.

Zeitgleich mit der Inbetriebnahme der Visa-Warndatei wurde ein Verfahren für einen Abgleich von bestimmten Daten aus dem Visumverfahren für Sicherheitszwecke gestartet. In diesem Datenabgleichverfahren werden in einer eigenen Organisationseinheit beim BVA Daten aus dem Visumverfahren mit bestimmten Daten aus der Antiterrordatei (ATD) automatisiert abgeglichen. Durch den automatisierten Abgleich wird eine Rückmeldung durch Sicherheitsbehörden an die Visumbehörden ermöglicht, wenn Personen, die dem vom ATD dem terroristischen Umfeld zugerechnet werden, nach Deutschland einzureisen versuchen. Auf diese Weise soll den sicherheitspolitischen Interessen im Visumverfahren Rechnung getragen werden (Bundesministerium des Innern, PM 05.06.2013, Visa-Warndatei nimmt Betrieb auf).

### Bund/Länder

## Polizei ermittelt Autobahnschützen mit Kfz-Kennzeichenerfassung und Funkzellenkontrolle

Eine Serie von Schüssen auf deutschen Autobahnen ist mithilfe monatelanger und millionenfacher Kennzeichen-Erfassung aufgeklärt worden. Der Präsident des Bundeskriminalamtes (BKA), Jörg Ziercke, teilte mit, dass der am 23.06.2013 verhaftete mutmaßliche Autobahnschütze mindestens 762 Mal auf andere Lastwagen geschossen hat, meist auf Autotransporter. Er habe die Taten weitgehend gestanden und als Motiv „Frust und Ärger im Straßenverkehr“ angegeben. Die Serie begann 2008. Die Ermittler verstärkten ihren Ermittlungsaufwand, als am 10.11.2009 bei Schüssen auf der A3 bei Würzburg eine Autofahrerin am Hals getroffen und schwer verletzt worden war. Durch Vermessen des Tatortes und Berechnung des Schusswinkels war klar, dass die Kugel von oben eingeschlagen und offenbar aus einem hohen Fahrzeug im Gegenverkehr abgefeuert worden war. Die Ermittler ließen alle Handys feststellen, die zur Tatzeit eingebucht waren. Mal pausierte der Schütze wochenlang, mal feuerte er Dutzende Schüsse an einem Tag ab. Die Ermittler ließen mehr als tausend Fahndungsplakate drucken und lobten eine Belohnung aus. Der Einsatz eines polizeilichen Lastwagens voller Überwachungselektronik war ergebnislos. Im September 2012 wurde eine „Besondere Aufbauorganisation Transporter“ beim BKA eingerichtet. Zeitweise sollen hundert Beamte mit dem Fall befasst gewesen sein. Es wurden Geräte zur Kennzeichenerfassung gemietet. Diese seien, so das BKA, an sieben Autobahnabschnitten von Aachen Richtung Bayern und Baden-Württemberg eingesetzt worden. Wenn Lastwagen beschossen wurden, seien deren Bewegungsdaten mit denen anderer Wagen auf der Strecke in Verbindung gebracht worden. Wenn keine Schüsse gemeldet wurden, seien die Daten nach zehn Tagen ungelesen gelöscht worden. Im April 2013 führte die Maßnahme zum Erfolg: Innerhalb von 5 Tagen waren 6 Schüsse auf Lastwagen gemeldet worden. Hieraus wurden wahrscheinliche Fahrtstrecken und Tatorte rekonstruiert. Es wurde ein Zeitraum von 18 Minuten herausgefiltert, innerhalb derer der Täter an einer der Kennzeichenkameras vorbeigefahren sein musste. So fanden die Fahnder genau einen Lkw einer Spedition in Monschau in der Eifel (Nordrhein-Westfalen), der es zeitlich geschafft hätte, auch an den anderen Tatorten aus dieser Woche zu sein. Die Überwachungsbilder wurden ausgewertet. Zudem sei überprüft worden, ob dessen Handy zu den fraglichen Zeiten in Funkzellen entlang der Autobahn eingeloggt war.

Bei dem verhafteten 57 Jahre alten Lkw-Fahrer seien zwei Pistolen und ein Schießkugelschreiber sichergestellt worden, sagte Ziercke. Man habe

noch 1.300 Schuss Munition gefunden. Der Würzburger Staatsanwalt Dietrich Geuder kündigte an, der 57-Jährige werde sich unter anderem wegen versuchten Totschlags verantworten müssen. Vor einigen Jahren soll ein Autotransporter den Lkw-Fahrer geschnitten und beinahe einen Unfall verursacht haben. Der mutmaßliche Schütze, ein „frustrierter Einzelgänger mit einem Hass auf andere Menschen und einer Affinität zu Waffen"", habe von einem „Krieg" auf deutschen Autobahnen gesprochen. Seine Taten sehe er als eine Art Selbstjustiz an. Er habe stets nur Gegenstände beschädigen, nie jemanden verletzen wollen, soll der Verdächtige gesagt haben.

Bayerns Innenminister Joachim Herrmann (CSU) lobte den Fahndungserfolg. Bundesinnenminister Hans-Peter Friedrich dankte dem BKA und sieht in der Überführung des Täters einen Erfolg länderübergreifender Zusammenarbeit des BKAs mit den Polizeien in Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz. Der Vorsitzende der Deutschen Polizeigewerkschaft, Rainer Wendt, sprach von einer „kriminologischen Meisterleistung".

Der rheinland-pfälzische Datenschutzbeauftragte Edgar Wagner hält den längerfristigen Einsatz von Kennzeichen-Lesegeräten entlang ganzer Autobahnabschnitte dagegen für zweifelhaft. Es gebe „für diese bundesweit erstmals eingesetzte Ermittlungsmethode aus Datenschutzsicht keine hinreichende gesetzliche Ermächtigungsgrundlage." Ziercke wies den Vorwurf zurück, die Ermittler seien unverhältnismäßig vorgegangen: „Es gab keine unkontrollierte Datensammelei. Wir haben die berühmte Nadel im Heuhaufen gefunden." Die Tatserie hätte mit Hilfe der Autobahn-Mautdaten früher beendet werden können. Gemäß Ziercke hat die Polizei mit großem Aufwand Daten sammeln müssen, die eigentlich bei der Lkw-Maut Toll Collect vorlägen: „In bestimmten Einzelfällen wäre es angemessen, diese Daten zu nutzen. Dafür müssten die Gesetze geändert werden. Ich möchte mal den Datenschützer sehen, der mit der Begründung, wir hätten das nicht zur Gefahrenabwehr nutzen dürfen, irgendjemanden überzeugen würde." Toll Collect erfasst mit rund 300 Anlagen die Kennzeichen von LKWs zu Zwecken der Gebührenabrechnung, wies aber die Anfragen der Ermittler ab.

Wagner lobte die Löschung der Kennzeichendaten nach 10 Tagen, kritisierte aber im Grundsatz die gesamte Maßnahme: „Millionen von unverdächtigen Personen geraten ins Visier der Ermittlungsbehörde, um einen Verdächtigen zu überführen." Seinen Berechnungen nach wurden seit Dezember 60 bis 80 Millionen Datensätze unverdächtiger Menschen erfasst. Er bestätigte, dass die Ermittler ihn vorher über den neuen Ansatz informiert haben. Er habe Bedenken geäußert, deshalb sei die Zehn-Tage-Regelung vereinbart worden. Er habe über den Vorgang auch in Ausschüssen des rheinland-pfälzischen Landtags berichtet (Datenschützer kritisieren Methode der Sniper-Fahndung, www.zeit.de 25.06.2013; Jekat, Lkw-Fahrer schoss aus Frust im Straßenverkehr, www.sueddeutsche.de 25.06.2013; PE BMI 25.06.2013; Martin-Jung/ Schneider, Jedes Kennzeichen im Visier, SZ 26.06.2013, 10; Ulrich, Der Frust des Fahrers, Der Spiegel 27/2013, 39).

### Bayern

## Fragwürdige polizeiliche Handyauswertung

Die Münchner Polizei muss sich in einem Fall wegen der umfangreichen Auswertung eines Handys einer 23-jährigen Frau rechtfertigen, die zuvor in einer Haftzelle geschlagen und schwer verletzt worden war. Das Handy wurde beschlagnahmt, um die Daten darauf hin auszuwerten, ob die Frau Kontakte in die Drogenszene hatte. Zusätzlich suchte die Polizei nach Kontakten zu den Medien. So wurde der SMS- und E-Mail-Verkehr zwischen der Frau und einem Münchner Journalisten kopiert, besonders markiert und zu den Ermittlungsakten genommen, obwohl es darin keinerlei Bezug zu den eigentlichen Ermittlungen gab. Die richterliche Anweisung gab den Ermittlern hierfür keine Erlaubnis. Oberstaatsanwalt Thomas Steinkraus-Koch erklärte: „Wir haben keinen Auftrag gegeben, das Handy auf Pressekontakte zu überprüfen." Das Innenministerium und das Polizeipräsidium lehnten jede Stellungnahme ab. Polizeisprecher Wolfgang Wenger sprach von „laufenden Ermittlungen".

Das Ermittlungsverfahren gegen einen 33-jährigen Polizeibeamten ist abgeschlossen, der die Frau in einer Haftzelle am 20.01.2013 schwer verletzt haben soll, so dass diese eine Nasenbeinfraktur erlitt. Gegen die Frau wird wegen Beleidigung und Widerstands sowie wegen Körperverletzung ermittelt, nachdem sie Polizisten beschimpft, getreten und bespuckt haben soll. Um herauszufinden, ob die Frau damals unter Drogen gestanden haben könnte, durchsuchte die Polizei am 15.02.2013 morgens um 6 Uhr die Wohnung der Frau, schnitt ihr in der Rechtsmedizin ein Büschel Haare ab und beschlagnahmte mit richterlichem Beschluss ihr Handy. Die Auswertung der Handy-Daten sollte sich beschränken auf „mögliche Verstöße gegen das Betäubungsmittelgesetz im tatrelevanten Zeitraum", um die Schuldfähigkeit der Frau an jenem Tag zu überprüfen.

So wurde der Journalist einer Münchner Tageszeitung, der über den Fall der Frau berichten wollte, unfreiwillig Gegenstand polizeilicher Ermittlungen. Name und Medium wurden vom Sachbearbeiter der Polizei mit gelbem Leuchtmarker angestrichen. In der polizeilichen Ermittlungsakte wurde erfasst, was er der Frau per SMS mitgeteilt hatte; und auch, was er ihr von seinem dienstlichen E-Mail-Account geschickt hat, fand Einzug in die polizeiliche Ermittlungsakte (Wimmer/ Krügel, Ermittlungen in der Grauzone, SZ 01./02.2013, 41).

### Bayern

## Telefonüberwachung bei Münchner Kripo-Dienststelle

Fast 30 Jahre lang sind im Münchner Polizeipräsidium Telefonapparate von Beamten des Kriminaldauerdienstes (KDD) überwacht worden. An vier Apparaten der Kripo-Dienststelle wurden Gespräche mitgehört und aufge-

zeichnet. Die Belegschaft war darüber überhaupt nicht oder nur unzureichend informiert. Die GesprächsteilnehmerInnen am anderen Ende der Leitung hatten keine Ahnung, dass sie überwacht wurden. Erst als sich ein Beamter Ende Juni 2013 beschwerte und mit einer Klage gedroht wurde, flog die „Abhöraffäre" auf. Das Präsidium rechtfertigte das Vorgehen mit Strafverfolgung und Gefahrenabwehr.

Es ist gesetzlich vorgesehen, dass eingehende Notrufe bei Polizei, Feuerwehr oder Rettungsdienst aufzuzeichnen sind. Wer 110 wählt, muss davon ausgehen, dass das Gespräch mitgeschnitten wird. Durch die Aufzeichnung werde, so die Münchner Polizei, „eine sichere und vollständige Übermittlung der gegebenenfalls ungenauen, lückenhaften und unverständlichen Informationen gewährleistet". Beim KDD wurde aber nicht nur die 110 überwacht; betroffen waren auch andere Gespräche in der Einsatzzentrale und sonst beim KDD. Gut 90 BeamtInnen sind in der Dienststelle tätig. Sie übernehmen während der Nachtstunden alle relevanten kriminalpolizeilichen Aufgaben. Die meisten BeamtInnen wussten nicht, dass die vier Apparate abgehört werden. So wurden auch private Gespräche ahnungsloser Beamter aufgenommen. Das Münchner Polizeipräsidium verwies darauf, dass man ähnlich wie in der Einsatzzentrale auch beim KDD Gespräche entgegennehmen müsse, die „polizeiliches Handeln erforderlich machen können". Das polizeiliche Aufgabengesetz sehe vor, dass außerhalb der Notrufeinrichtungen aufgenommen werden darf, „soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist; auf die Aufzeichnung soll hingewiesen werden".

Ungeklärt blieb zunächst, ob über diese Nebenstellen beim KDD auch Gespräche mit Berufsgeheimnisträgern wie Rechtsanwälten, Staatsanwälten oder Richtern entgegengenommen und vertrauliche Inhalte aufgezeichnet wurden. Nach der Beschwerde eines Beamten, wurden die Mitschnitte zunächst fortgeführt. Erst als mit einer Klage gedroht wurde, lenkte das Präsidium ein und stoppte die Daueraufnahmen. Strafverteidiger Marco Noli bewertete die Aufzeichnungen als „Misstrauen gegenüber den Mitarbeitern, Vertrauensbruch gegenüber dem Bürger und Verdacht einer Straftat." Michael Hinrichsen, stellvertretender Landesvorsitzender der Deutschen Polizeigewerkschaft (DPolG) meinte: „Wenn tatsächlich beim Kriminaldauerdienst permanent die Gespräche auf vier Apparaten mitgeschnitten wurden und die Kollegen nichts wussten, dann verurteile ich das aufs Schärfste." Susanna Tausendfreund, Landtagsabgeordnete der Grünen, forderte parlamentarische Aufklärung. Der Landesbeauftragte für Datenschutz, Thomas Petri, geht der Sache nach. Wenn das Präsidium keine Befugnis hatte, die Gespräche mitzuschneiden, so Petri, „dann liegt eine Straftat vor" (Wimmer, Lauschangriff bei der Münchner Polizei u. Wer überwacht die Überwacher?, www.sueddeutsche.de, 08.07.2013; Wimmer, Abhöraffäre bei der Polizei, SZ 08.07.2013, 24).

### Bayern

## Bespitzelung einer Whistleblowerin bei Edeka Südbayern

Das Einkaufszentrum Westpark am Rande von Ingolstadt gehört zu Edeka Südbayern, eine von sieben Gesellschaften im bundesweiten Genossenschafts-Verbund. Bei Edeka Südbayern rumort es; von Korruption, internen Intrigen, Einschüchterungen und der Bespitzelung von Mitarbeitern war immer wieder die Rede. Nun scheint eine Mitarbeiterin – ausgerechnet die Tochter eines Edeka-Topmanagers – ausspioniert worden zu sein. In einem sechsseitigen Brief an Geschäftsführung und Aufsichtsräte von Edeka Südbayern erhob dieser Manager schwere Vorwürfe gegen die eigene Organisation. Nachdem seine Tochter „dubiose Auftragsvergaben an Handwerker und Firmen" durch den Westpark-Leiter intern angezeigt habe, sei sie schikaniert und bespitzelt worden.

Entgegen seinen Zusicherungen und den eigenen Richtlinien soll der Compliance-Beauftragte der Edeka Südbayern die Hinweise der Frau nicht vertraulich behandelt haben. Die Firma habe die Mitarbeiterin und Managertochter, die bis dahin zehn Jahre untadelig im Unternehmen gearbeitet habe, zuletzt als Assistentin des von ihr beschuldigten Westpark-Chefs, im Stich gelassen. Im Gegenzug soll der Chef alles daran gesetzt haben, seine Mitarbeiterin loszuwerden. Er warf ihr plötzlich vor, mehr Arbeitszeit abzurechnen als tatsächlich zu leisten. Mit Videoüberwachung im Einkaufszentrum soll er die Frau bespitzelt und Bewegungsprofile von ihr erstellt haben. Zu diesem Zweck habe er eigens den Aufnahmewinkel einer Kamera verändern lassen. Die Mitarbeiterin sei beobachtet worden, wann sie ins Büro kam und wann sie es verließ.

Die Vorwürfe des Vaters, selbst ein ranghoher Manager bei der Edeka Südbayern, führten dazu, dass diesem selbst als Quittung Ende Juni 2013 fristlos gekündigt wurde. Der beschuldigte Westpark-Leiter erklärte, er erwäge rechtliche Schritte gegen den Vater und wolle sich deshalb nicht äußern. An Stelle der Geschäftsführung äußerte sich der Bielefelder Rechtsanwalt Carsten Thiel von Herff, der als Ombudsmann der Edeka Südbayern mit dem Fall befasst ist, und wies die Vorwürfe des Vaters als „falsch" zurück. Es habe „hinreichende Anhaltspunkte" für Unregelmäßigkeiten bei den Arbeitszeiten der Mitarbeiterin gegeben. Daraufhin habe der Westpark-Leiter „die Aufzeichnung einer Kamera ausgewertet", die eigentlich aus Sicherheitsgründen in einem der öffentlichen Zugänge zum Einkaufszentrum angebracht sei.

Das bayerische Landesamt für Datenschutzaufsicht hat den Vorgang geprüft und kam zu dem Ergebnis, dass „die Auswertung der zweckgebundenen Videoaufzeichnungen im Hinblick auf arbeitsrechtliche Verstöße" unzulässig war. Das Persönlichkeitsrecht der Mitarbeiterin sei verletzt worden. Bloße Hinweise auf falsche Angaben von ihr bei der Abrechnung von Arbeitsstunden seien kein ausreichender Grund, um ein Bewegungsprofil aus Videoaufzeichnungen zu erstellen: „Unserer Ansicht nach fehlt es an der Erforderlichkeit der Datennutzung." Die Edeka Südbayern erteilte gegen die Mitarbeiterin wegen der angebli-

chen Arbeitszeitmanipulationen eine Abmahnung, die sie aber später wieder zurücknahm, so Ombudsmann Thiel von Herff, „nicht aus rechtlichen Gründen, sondern lediglich auf meine Empfehlung, um zu deeskalieren“. Gemäß internen Unterlagen war er aber noch wenige Monate zuvor zu einem etwas anderen Ergebnis gekommen: Ob die Abmahnung begründet sei, könne er nicht sicher bewerten, hieß es damals, unverhältnismäßig sei sie in jedem Fall. Eine mündliche Ermahnung – das mildere Mittel als die Abmahnung – hätte es auch getan. Am Vorgehen von Edeka findet der Ombudsmann wenig auszusetzen. Der Vorwurf, ein Edeka-Beauftragter habe die Angaben der Mitarbeiterin über Missstände nicht vertraulich behandelt, sei falsch. Ihr Name werde zwar neben dem anderer Westpark-Beschäftigter genannt, aber nicht als Hinweisgeberin. Immerhin gingen die Edeka-Revisoren den Angaben der Frau nach und stießen gemäß einem internen Sonderprüfungsbericht tatsächlich auf fragwürdige Auftragsvergaben und äußerten den „Verdacht einer bevorzugten Behandlung“ bestimmter Firmen; manche Verflechtungen seien „sehr sonderbar und abschließend nicht vollständig erklärbar“. Als Konsequenz erhielt der Westpark-Chef einen Stellvertreter an seine Seite gestellt (Läsker/Ritzer, Eine Welt für sich, SZ 29./30.06.2013, 28).

### Hamburg

## Kreditech vergibt Online-Kredite nach Social Scoring

Kreditech ist ein Startup aus Hamburg-Winterhude, das Geld über das Internet verleiht und zwar Minikredite. Die maximal verliehene Summe sind 500 Euro; der Durchschnittskunde erhält 109 Euro. Firmengründer sind Sebastian Diemer und Alexander Graubner-Müller. Kreditech verlangt keine Schufa-Auskunft, sondern ermittelt die Ausfallwahrscheinlichkeit selbst über ein Social-Scoring-Verfahren auf der Grundlage u. a. von Internet-Datenanalysen, so Diemer: „Im Idealfall ist das Geld innerhalb von 15 Minuten nach Bewilligung auf dem Konto; in Polen klappt das schon regelmäßig.“ Das Unternehmen fordert so viele Daten wie irgend möglich; je mehr es erhält, umso präziser wird die Prognose und desto höher liegt der Kreditrahmen für die Kunden.

Datengrundlage sind die ohnehin öffentlich einsehbaren Bewertungsprofile von Ebay-Konten oder die Profile bei Facebook sowie weiteren Plattformen, z. B. Xing oder LinkedIn. Es wird u. a. geprüft, ob Foto und Ort mit Informationen bei den Netzwerken übereinstimmten und ob es unter den Freunden viele mit ähnlichen Bildungsabschlüssen gibt oder viele Kollegen, die in derselben Firma arbeiten. Dies erhöhe die Wahrscheinlichkeit, es mit einer realen Person zu tun zu haben. In die Wertung einbezogen wird auch, ob die Kreditbitte von einem teuren iPad oder von einem billigen Aldi-Computer ausging. Eine Rolle spielt auch das Online-Verhalten des Antragstellers, z. B. die Zeit, die zum Ausfüllen des Fragebogens benötigt wird, oder die Fehlerhäufigkeit und der Einsatz der Löschtaste. Nach Angaben der Macher werden bis zu 8.000 Einzelinformationen vom Kreditech-Algorithmus verarbeitet. Die im März 2012 gegründete Firma expandierte schnell. Sie ist in Polen, Spanien und Tschechien online. In Russland ist der Start im Juni 2013 vorgesehen. In Deutschland lief der Geldverleih 3 Wochen lang. Dann stellte Kreditech „präventiv“ den Service ein, wohl weil sich die deutsche Finanzaufsicht BaFin meldete und die Prüfung des Geschäftsmodells ankündigte, u. a. wegen der hohen Zinsen und der Pflicht, ein „Bonitätszertifikat“ für bis zu 49 Euro zu erwerben. Der Zertifikatserwerb wurde inzwischen nach Firmenangaben wieder auf allen Märkten abgeschafft. Die verlangten Zinsen sind von Darlehenshöhe, Scorewert und Laufzeit abhängig und betragen zwischen 5 und 28% pro Monat.

Das Geschäftsmodell zielt nicht nur auf die Zinseinnahmen, sondern auch auf den Aufbau einer internationalen, sich selbst aktualisierenden Bonitätsdatenbank, die durch andere Unternehmen, insbesondere Online-Händler, genutzt werden soll. Anders als bisherige Scoring-Verfahren, z. B. der Schufa, die auf wenigen Parametern basieren, die insbesondere auf die Kreditvergangenheit Bezug nehmen, werden viele weitere Datensätze einbezogen. Grabner-Müller erläutert: „Für fast drei Viertel der Weltbevölkerung gibt es noch keine verlässlichen Bonitätsauskünfte.“ In vielen Ländern gibt es keine ähnliche große Marktdurchdringung von Bonitätsauskunfteien wie in Deutschland. Neben Kreditech gibt es andere Anbieter wie Zestfinance oder das britische Wonga, die ähnliche Ziele in prekären Märkten verfolgen. In Großbritannien machte Wonga Negativschlagzeilen, als es versuchte, Studierende aus staatlichen Studentenkrediten in eigene ungleich teurere Darlehen zu locken.

Die Kreditech-Gründer behaupten, man habe sich weder in Sachen Datenschutz noch bei der Zinshöhe etwas vorzuwerfen: „Die Schufa speichert Daten auf Vorrat, wir nur bei einer konkreten Anfrage.“ Im Übrigen würden die Daten abgelehnter Antragsteller nach 90 Tagen fast sämtlich gelöscht; nur was notwendig sei, um einen einmal abgelehnten Bewerber wiederzuerkennen, werde länger vorgehalten. Investoren halten Social Scoring für außerordentlich attraktiv. So sicherte sich Kreditech im Dezember 2012 4 Mio. Dollar Risikokapital; im April 2013 stiegen die Samwer-Brüder mit einem Fonds in ähnlicher Höhe ein. Wonga sammelte bereits 141 Mio. Dollar von Geldgebern (Müller/Rosenbach/Schulz, Die gesteuerte Zukunft, Der Spiegel 20/2013, 72).

### Hamburg

## Bußgeld gegen Google wegen WLAN-Scanning

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat gegen Google Inc. wegen unzulässiger WLAN-Mitschnitte ein Bußgeld von 145.000 Euro verhängt. Von 2008 bis 2010 hatte Google nicht nur Straßen und Häuser für den Dienst Google Street View fotografiert, sondern auch WLAN in Reichweite der dabei verwendeten Fahrzeuge erfasst. Dabei wurden auch Inhaltsdaten

der erfassten unverschlüsselten WLAN-Anschlüsse aufgezeichnet. Unter den im Vorbeifahren erfassten Informationen befanden sich auch erhebliche Mengen an personenbezogenen Daten unterschiedlichster Qualität, z. B. E-Mails, Passwörter, Fotos und Chat-Protokolle.

Nachdem der Sachverhalt im Jahre 2010 aufgedeckt wurde, eröffnete die Staatsanwaltschaft Hamburg ein Ermittlungsverfahren, das im November 2012 eingestellt wurde. Der HmbBfDI hat daraufhin ein Bußgeldverfahren wieder aufgegriffen und abgeschlossen. Mit dem Bußgeldbescheid wurde Google zugleich angewiesen, die unzulässig erhobenen Daten vollständig zu löschen, was dem HmbBfDI gegenüber von Google bestätigt wurde.

Nach Ansicht des HmbBfDI Johannes Caspar zeigen Fälle wie dieser deutlich, dass die Sanktionen, die das Bundesdatenschutzgesetz vorsieht, für die Ahndung derartig schwerwiegender Datenschutzverstöße nicht ausreichen. Für multinationale Konzerne sei ein Bußgeld bis zu 150.000,- Euro für fahrlässige, bis zu 300.000,- Euro für vorsätzliche Verstöße regelmäßig ohne abschreckende Wirkung: „Solange Datenschutzverstöße nur zu Discount-Preisen geahndet werden können, ist die Durchsetzung des Datenschutzrechts in der digitalen Welt mit ihren hohen Missbrauchspotentialen kaum möglich. Die derzeit im Zuge der künftigen europäischen Datenschutzgrundverordnung diskutierte Regelung, die als maximales Bußgeld 2% des Jahresumsatzes des Unternehmens vorsieht, würde dagegen eine wirtschaftlich spürbare Ahndung von Datenschutzverletzungen ermöglichen“ (PE HmbBfDI 22.04.2013).

### Hessen

## Acxiom bietet Personenprofile zu Religion und Ethnie

Acxiom, einer der größten Daten-Analysten der Welt, sammelt und verkauft in Deutschland personenbezogene Daten zur ethnischen Herkunft von rund 15 Millionen Menschen. Das Wirtschaftsmagazin ‚Capital‘ (Ausgabe 7/2013) berichtet, dass Acxiom dabei auch Profile zur Religionszugehörigkeit von BürgerInnen bildet und diese ohne ihr Wissen und ohne ihre Einwilligung etwa als „außereuropäisch-islamisch“ einstuft. Weitere Kategorien der Daten-Profile sind „Spätaussiedler“, „Balkan“ oder auch „afrikanisch / südlich der Sahara“.

Die personenbezogenen Datenprofile verkauft Acxiom weltweit an Interessierte, so deren Broschüre zum „Ethno-Marketing“: „Wer weiß, wo die unterschiedlichen ethnischen Gruppen wohnen, ist klar im Vorteil.“ Die Zugehörigkeit einer Person zu einem Kulturkreis werde auf der Basis einer Vor- und Nachnamens-Analyse identifiziert und mit amtlichen Informationen zur Anzahl der Ausländer abgeglichen. Für jeden Straßenabschnitt Deutschlands könne, so Acxiom über sich selbst, die Zugehörigkeit zu zehn Kulturkreisen ausgewiesen werden. Auf Wunsch von Kunden werde „die ethnische Herkunft auch auf Personen-Ebene“ ausgewiesen, also mit Name und Adresse. Erkenntnisse aus der Analyse könnten damit „sofort vertrieblich nutzbar gemacht werden“, etwa für Postwurfsendungen oder zur „Selektionen kulturkreisbezogener Zielgruppenadressen“.

Der für Acxiom Deutschland zuständige Hessische Datenschutzbeauftragte zeigte sich verwundert, so dessen Mitarbeiter Ralf Menger: „Solange sich die Datenverarbeitung nur an einen Sprachraum knüpft, ist das zulässig, aber Kriterien wie ‚islamisch‘ und ‚Spätaussiedler‘ sind sehr fragwürdig, da Daten zur Religion und zur Ethnie nur mit Einwilligung der Betroffenen genutzt werden dürfen. Wir werden jetzt prüfen, welche Daten Acxiom verarbeitet.“ Bereits vor fünf Jahren habe man mit Acxiom über das Ethno-Marketing gesprochen, doch die rechtlich problematischen Kriterien habe es damals noch nicht gegeben. Der Geschäftsführer von Acxiom Deutschland, Carsten Diepenbrock, wies die Vorwürfe zurück; das „Ethno-Marketing“ sei aus Sicht des Unternehmens datenschutzrechtlich einwandfrei (Thieme, Datensammler bieten Personenprofile zu Religion und Ethnie: Datenschützer wollen Rechtmäßigkeit prüfen, www.presseportal.de 20.06.2013).

### Niedersachsen

## Kommunalsteuerdaten von Schneverdingen abhandengekommen

Die Stadt Schneverdingen hat Namen, Anschriften und sogar die Bankdaten von rund 8.000 EinwohnerInnen an eine Berliner Softwarefirma weitergegeben, um einen Fehler aufzuspüren. Der Computer inklusive Daten wurde dort bei einem Einbruch geklaut. Mit der Kombination von Name und Bankdaten ließen sich Online-Einkäufe tätigen und ganze Konten über Lastschriftverfahren abräumen. Der Niedersächsische Landesbeauftragte für Datenschutz (LfD Nds) hat eine Prüfung begonnen. Die Stadt ist sich keiner Schuld bewusst, so Walter Rieser aus der Finanzverwaltung: „Uns ist das hochunangenehm.“ Doch der Fehler liege bei der Softwarefirma in Berlin, die die Daten nicht, wie vertraglich geregelt, direkt nach dem Transfer vom Laptop gelöscht habe. Der Vertrag habe auch sichergestellt, dass die Verschlüsselung von Daten und Leitung höchsten Sicherheitsstandards entspreche. Um welche Art der Verschlüsselung es sich dabei handelt, konnte Rieser allerdings nicht sagen. Michael Knaps, Pressesprecher des LfD Nds, kommentierte: „Da stellt sich die Frage, ob eine private Firma diese Daten überhaupt sehen darf.“ Gängiger sei es im Bereich von Softwareproblemen, mit Dummies zu arbeiten. Für Schneverdingen war das keine Option. Gemäß Bürgermeisterin Meike Moog-Steffens (SPD) habe der Hersteller der fehlerhaften Finanz-Software aus der Ferne nicht klären können, ob der Zusammenbruch des Systems auf einen Defekt in der Anwendung oder im Datensatz zurückzuführen sei: „Die brauchten Echtdaten von uns.“

Als die Berliner Firma um die Übermittlung dieser Daten bat, habe sich die Stadt sofort mit dem LfD Nds in Verbindung gesetzt, so Moog-Steffens: „Dort haben wir erfragt, wie wir in diesem Fall vorzugehen haben. Wir haben uns natürlich abgesichert.“ Auf Grundlage dieser Auskünfte sei dann ein Vertrag mit der Berliner Firma aufgesetzt worden, um einen rechtlich korrekten Datentransfer zu gewährleisten.“

Von einem solchen Gespräch, geschweige denn einer offiziellen Anfrage der Schneverdinger, weiß man in Hannover beim LfD Nds jedoch nichts, so Knaps: „Wir wurden nach dem Verlust der Daten informiert.“ Dies sei erfreulicherweise unmittelbar nach dem Diebstahl geschehen. Dass aber einer seiner Kollegen die Transaktion im Vorwege abgenickt habe, kann er sich nur schwer vorstellen (Mennen, Schneverdingen nach dem Datenklau, http://www.ndr.de 06.05.2013).

# Datenschutznachrichten aus dem Ausland

### International/Bayern

## Patentamtsbelegschaft streikt gegen übermäßige Kontrolle

Angestellte im Europäischen Patentamt (EPA) traten am 26.06.2013 im Interesse ihrer Menschenwürde und ihres Streikrechts in den Ausstand. Das EPA beschäftigt 7.000 Mitarbeitende, 4.000 davon in München. Zu der Demonstration an diesem Tag waren viele auch von den Standorten Den Haag, Berlin und Wien angereist. Anlass für die Proteste war eine Verschärfung des Personalstatuts. Darüber verhandelte auf Vorschlag von EPA-Präsident Benoît Batistelli am 26. und 27.06.2013 der Verwaltungsrat, das oberste Gremium der von 38 Staaten getragenen Organisation. Einer der für vertraulich erklärten Beschlussvorlagen zufolge werden Angestellte nach einer Krankmeldung verpflichtet, zwischen 10 und 12 sowie 14 und 16 Uhr zu Hause zu sein. Der Präsident darf danach ihnen einen Arzt schikken, der sie in der Wohnung untersucht. Weigern sich die Angestellten, gilt ihre Krankheit als vorgeschoben. Die Mitarbeitenden selbst sehen in den geplanten Regelungen hingegen ein „unwahrscheinliches Misstrauen“, wie ein Demonstrant vor dem EPA sagte. „Dahinter steht der Glaube: Das Personal macht blau.“ Als Beschäftigte einer internationalen Organisation haben sie ansonsten viele Privilegien und erhalten ihre hohen Gehälter steuerfrei.

Die Patentamts-Leitung begründete die Maßnahmen mit einem im Vergleich zu anderen internationalen Organisationen um 30% höheren Krankenstand. EPA-Sprecher Oswald Schröder erläuterte: „Dass wir einen Arzt zu einem kranken Mitarbeiter schikken, wird aber die absolute Ausnahme bleiben.“ Die Behörde unterliegt nicht dem deutschen Arbeitsrecht und muss sich deshalb eigene Regeln geben. Das Bundesjustizministerium, das die deutsche Delegation im Verwaltungsrat stellt, zeigte sich zugeknöpft: „Das sind Personalangelegenheiten, die wir im Verwaltungsrat besprechen werden.“ Nach Ansicht der Münchner Anwältin Senay Okyay in einem Gutachten für die SUEPO, der Gewerkschaft der EPA-Angestellten, verstoßen die Regeln für die Krankschreibungen gegen etliche Grundrechte. Menschenwürde, freie Arztwahl und Unverletzlichkeit der Wohnung seien nicht nur in Deutschland garantiert, sondern in allen Mitgliedsstaaten des Patentamts. Angestellte selber äußerten sich dazu nur anonym, weil sie Disziplinarmaßnahmen fürchten, so eine Mitarbeiterin: „Wer als Erster den Mund aufmacht, ist der Erste, der fliegt.“

Auch Änderungen beim Streikrecht empörten EPA-Angestellte. Zwar räumte der Entwurf aus Batistellis Büro Angestellten dieses Recht ein. Zugleich sichert es dem Präsidenten die Kontrolle. Das Amt organisiert die Urabstimmung. Abstimmen dürfen alle Mitarbeiter, nicht nur Gewerkschaftsmitglieder; wer teilnimmt, wird in der Chefetage registriert. Batistelli hatte nicht vor, den Verwaltungsrat mit den Details zu befassen. Das gilt sowohl für die geforderte Anwesenheit zu Hause im Krankheitsfall als auch für die Hoheit über die Urabstimmung. Eine vorbereitete Richtlinie verbietet andere Arbeitskampfmaßnahmen, etwa den Dienst nach Vorschrift ohne jegliche Eigeninitiativen (Schrader, Blaumachen, bis der Arzt kommt, SZ 26.06.2013, 1; Europäisches Patentamt: Mitarbeiter streiken, www.abendzeitung-muenchen.de 26.06.2013; Stoffels, Ausstand der Belegschaft des Europäischen Patentamts in München, http://blog.beck.de 05.07.2013).

### Österreich

## Neue Datenschutzbehörde übernimmt Aufgaben der Datenschutzkommission

Der österreichische Gesetzgeber hat die Novelle des Datenschutzgesetzes beschlossen, welche die Einrichtung einer neuen unabhängigen Datenschutzbehörde vorsieht. Diese wird nicht nur als Kontrollstelle zur Überprüfung der Einhaltung von Datenschutzvorschriften fungieren, sondern unter anderem auch für die Führung von Registrierungsverfahren, die Genehmigung von Datenübermittlungen ins Ausland, die Genehmigung von Datenverwendungen für wissenschaftliche oder statistische Zwecke und die Auskunftserteilung an BürgerInnen zuständig sein. Der Leiter bzw. die Leiterin der Datenschutzbehörde soll für jeweils fünf Jahre vom Bundespräsidenten auf Vorschlag der Regierung bestellt werden.

Bescheide der neuen Datenschutzbehörde können beim Bundesverwaltungsgericht angefochten werden, wobei die Entscheidungen dort ein Senat unter Einbindung fachkundiger

LaienrichterInnen aus dem Kreis der Arbeitgeber und der Arbeitnehmer treffen wird. Ein jährlich zu erstellender Bericht der Datenschutzbehörde soll auch dem Nationalrat und dem Bundesrat übermittelt werden.

Von der ursprünglich vorgesehenen Einrichtung eines Fachbeirats zur Unterstützung der Datenschutzbehörde wurde letztendlich abgesehen. Man wolle jeglichen Zweifel an der Unabhängigkeit der Datenschutzbehörde vermeiden, hieß es dazu in den Erläuterungen zu einem am 19.04.2013 gemeinsam von SPÖ, ÖVP und FPÖ vorgelegten Abänderungsantrag. Außerdem wurde durch eine Umformulierung des Gesetzentwurfs deutlicher sichtbar gemacht, dass nicht nur öffentliche Auftraggeber in Verfahren vor der Datenschutzbehörde Parteistellung erhalten. Der Datenschutzrat erhält die ausdrückliche Erlaubnis, Gutachten zu Fragen von grundsätzlicher Bedeutung des Datenschutzes einzuholen (Verfassungsausschuss billigt Novellierung des Datenschutzgesetzes, www.ots.at 16.04.2013).

### Frankreich

## Vorwürfe gegen Auslandsgeheimdienst wegen Massendatenkontrolle

Nach den Enthüllungen durch Edward Snowden über die Überwachungsaktivitäten der US-amerikanischen und der britischen Sicherheitsbehörden berichtete die französische Zeitung „le Monde" am 05.07.2013, dass der dortige Auslandsgeheimdienst, die „Direction Générale de la Sécurité Extérieure" (DGSE) in ähnlicher Art und Weise Kommunikationsdaten abgreift und auswertet. „Unsere gesamte Kommunikation wird ausspioniert." Die DGSE fange Signale von Computern und Telefonen in Frankreich ab. Betroffen seien auch Verbindungen zwischen Frankreich und dem Ausland. Zwar würden nicht die Inhalte von Gesprächen ausgeforscht. Vielmehr gehe es darum, eine Übersicht, eine Art Karte zu erstellen, wer mit wem kommuniziere. Der Pressebericht nimmt Bezug auf namentlich nicht genannte Geheimdienstquellen sowie offizielle Äußerungen von Geheimdienstmitarbeitern. Es handele sich um illegale Eingriffe. Anders als beim britischen Programm „Tempora" fehle es an jeder rechtlichen Kontrolle. E-Mails, SMS, Verbindungsdaten und die Nutzung von Facebook und Twitter etwa würden über Jahre gespeichert.

Gemäß dem Bericht speichert die DGSE die Milliarden Datensätze in den drei Etagen im Keller ihres Hauptquartiers in Paris am Boulevard Mortier. Die Wärme, die das Rechenzentrum ausstrahle, reiche aus, um das gesamte Gebäude zu heizen. Weitere sieben französische Dienste, darunter der Inland- und der Militärgeheimdienst, Experten für Geldwäsche, die Polizei und Zollfahnder, hätten Zugriff auf die Daten. Diesen anderen Diensten sei es dann freigestellt, sich in als verdächtig aufgefallene Kommunikation einzuklinken und etwa Gespräche abzuhören. Das offiziell nicht existierende Rechenzentrum habe inoffiziell den Namen „Infrastruktur für die wechselseitige Nutzung". Ziel sei es, den Terror zu bekämpfen. Zugleich könne aber das Kommunikationsprofil jedes Bürgers gezeichnet werden.

Die DGSE gab keine offizielle Stellungnahme ab. Die für die Kontrolle solcher Spionagemaßnahmen zuständige Kommission zweifelte die Berichte an und versicherte, der Geheimdienst arbeite im Einklang mit den Gesetzen. Die einzige Einrichtung, die Kommunikationsdaten sammle, sei eine Regierungsstelle, die dem Premierminister unterstellt sei und deren Aufgabe es sei, Sicherheitslücken aufzuspüren. Das Amt des Premierministers Jean-Marc Ayrault bezeichnete die Berichte als „nicht exakt". Es gebe „mehrere Dienste", die aus Sicherheitsgründen Daten abfingen, darunter der DGSE, der Inlandsgeheimdienst und der Zoll. Alle diese Spähmaßnahmen seien gesetzlich geregelt. Gemäß einem Gesetz aus dem Jahr 1991 schlage die Nationale Kontrollkommission dem Premierminister Spähmaßnahmen vor, die dieser dann autorisieren könne. Diese Maßnahmen würden dokumentiert und kontrolliert.

Der Sozialist Jean Jacques Urvoas, Vorsitzender des Rechtsausschusses der Nationalversammlung, warf der Zeitung „Phantastereien und Ungenauigkeiten" vor. Dass sämtliche Daten angezapft und gelagert würden, entspreche nicht der Realität, wie er sie kenne. Die Franzosen seien keineswegs einer massiven und dauerhaften Ausspionierung außerhalb jeder Kontrolle ausgeliefert. Während der US-Geheimdienst NSA mit dem „Schleppnetz" zu fischen scheine, fische die französische DGSE zielgenau mit der „Harpune".

Die Enthüllungen über das US-Spähprogramm „Prism", insbesondere Berichte über das Abhören von EU-Einrichtungen und nationalen Botschaften, hatten in Frankreich zu großer Empörung geführt. Staatschef François Hollande hatte gar die Verschiebung von Freihandelsverhandlungen mit den USA erwogen, sollten die USA den Europäern nicht „garantieren", dass sie ihre Spähaktivitäten einstellen. Dem gegenüber blieb das Echo auf die Vorwürfe von Le Monde verhalten. Zeitungen und Internetseiten berichteten zunächst überhaupt nicht oder auf hinteren Plätzen und versuchten die publizierten Recherchen zu widerlegen oder abzuschwächen.

Der Auslandsgeheimdienst DGSE untersteht dem Verteidigungsminister. Er ist in seiner heutigen Form 1982 gegründet worden und soll Informationen sammeln, die für das nationale Interesse Frankreichs von Bedeutung sind, etwa im Kampf gegen die Verbreitung von Massenvernichtungswaffen oder gegen Terroristen. Der Dienst verfügt über ein Jahresbudget von 600 Mio. Euro, mehr als hundert Standorte im Ausland und ungefähr 5.000 Mitarbeitende. Annähernd die Hälfte von ihnen soll für die technische Abteilung arbeiten, die Überwachungsprogramme organisiert (Ulrich, Harpune statt Schleppnetz, SZ 06./07.07.2013, 6; Wagner u. a., Auch Frankreichs Geheimdienst zapft massenhaft Daten ab, www.spiegel.de 04.07.2013; Frankreich soll massenhaft Internet-Kommunikation überwachen, www.sueddeutsche.de 05.07.2013).

Frankreich u. a.

## AXA will Internet nach (möglichen) KundInnen scannen

Der französische Axa-Versicherungskonzern will in großem Umfang das Internet durchsuchen, um zusätzliche Informationen über bestehende und künftige KundInnen zu gewinnen. Konzernchef Henri de Castries erläuterte: „Heute stellt ein Versicherer bei Vertragsschluss 27 oder 30 Fragen, dabei gibt es schon Tausende von Angaben über den Kunden im Internet und bei uns selbst.“ Die Auswertung der großen Datenmengen sei eine zentrale Herausforderung für die Branche. Es gebe Gespräche zwischen Axa und Google: „Google weiß schon so viel über die Menschen, damit könnte es auch Finanzdienstleistungen anbieten“. Für den „globalen Datenberg“ müssten die Regierungen dringend Aufsichtsregeln für alle Unternehmen beschließen, die den Datenschutz für die Betroffenen ausreichend berücksichtigten (SZ 01./02.06.2013, S. 30).

Großbritannien

## GCHQ bespitzelte G20-Gipfel im Jahr 2009

Kurz vor Beginn des G8-Gipfels in Lough Erne in Nordirland am 15./16.06.2013 berichtete die Presse unter Berufung auf Dokumente des Whistleblowers Edward Snowden über Überwachungsaktionen des britischen Geheimdienstes GCHQ im Rahmen des G20-Gipfeltreffens im September 2009 in London. Edward Snowden hatte kurz zuvor Details über das streng geheime Überwachungsprogramm Prism des US-amerikanischen Geheimdienstes National Security Agency (NSA) öffentlich gemacht. Unter anderem seien Computer überwacht und Telefonanrufe abgehört worden. Durchgeführt worden sei die Überwachung vom Government Communications Headquarters (GCHQ), dem britischen Gegenstück zum US-Geheimdienst NSA. Einige Delegationen seien dazu gebracht worden, ein Internetcafé zu nutzen, das zuvor vom Geheimdienst eingerichtet worden sei. Sämtliche Computer waren präpariert worden. So habe man den E-Mail-Verkehr überwachen und Passwörter erbeuten können, noch bevor die Mail-Empfänger die Nachricht gelesen hatten. BlackBerry-Mobiltelefone von Delegierten wurden gehackt, so dass nicht nur ein Zugriff auf Mails, sondern auch das Mithören von Telefonaten möglich war.

In dem Bericht heißt es, mit der Aktion habe die Regierung offensichtlich einen Verhandlungserfolg beim Gipfeltreffen sicherstellen wollen. Ziele von Spähattacken seien auch Delegationen langjähriger Verbündeter wie Südafrika oder der Türkei gewesen. Auch die Kommunikation des damaligen russischen Präsidenten Dmitri Medwedew mit seiner Delegation sei über eine Kooperation der NSA mit dem GCQH ins Visier geraten. Einige der Delegierten, die damals Ziel der Spionage waren, waren im Juni 2013 erneut Gast des G20-Gipfels. Rund 45 AnalystInnen sollen rund um die Uhr darüber informiert gewesen sein, wer mit wem telefonierte. In einem Briefing von Mitarbeitenden an den damaligen GCHQ-Chef heißt es: „Die Absicht der GCHQ ist es sicherzustellen, dass Informationen, die unserer Regierung helfen, ihre Ziele während der G20-Präsidentschaft zu erreichen, den Kunden zur richtigen Zeit erreichen, und zwar so, dass er sie bestmöglich einsetzen kann.“ Die Ergebnisse wurden auf einer 5 Meter breiten Schautafel präsentiert und ausgewertet. Der Geheimdienst sprach von einem dauernden „dynamischen Auswerten“ der Leitungen. Am Ende der Operation wurde in einer internen Überprüfung der Aktion deren Erfolg gelobt: „Es hat sich als nützlich herausgestellt zu notieren, welche nationale Delegation in der Zeit vor, während und nach dem Gipfel aktiv war. Alles in allem ein sehr erfolgreiches Wochenende mit der Telefonaktion gegen die Delegationen.“ Bescheid gewusst haben soll unter anderem der damalige Premierminister Gordon Brown von der Labour-Partei.

Die britische Regierung in der Downing Street von Premier David Cameron verkündete daraufhin, man äußere sich grundsätzlich nicht zu Sicherheitsfragen. Auch von den internationalen Delegierten in Nordirland gab es zunächst keine Reaktionen. Die türkische Regierung soll aber den britischen Botschafter in Ankara einbestellt haben. Der stellv. Sprecher der deutschen Bundesregierung Georg Streiter meinte, keine Informationen zu den Vorgängen zu haben (Lauschangriff: Großbritannien spionierte G-20-Delegierte aus, www.berliner-zeitung.de 17.06.2013; Zaschke, Beschnüffelte Gipfelgäste, SZ 18.06.2013, 7).

Großbritannien

## Wanze in Ecuadors Botschaft

Die ecuadorianische Botschaft in London, wo der Gründer des Enthüllungsportals Wikileaks, Julian Assange, Asyl fand, ist nach Angaben der Regierung in Quito abgehört worden. Außenminister Ricardo Patiño gab bekannt: „In den Büros von Botschafterin Ana Albán ist ein verstecktes Mikrofon gefunden worden.“. Die Wanze sei bei einer Überprüfung der Räumlichkeiten vor seinem Besuch in Großbritannien Mitte Juni entdeckt worden. Sie sei in einer Steckdose angebracht gewesen und konnte über eine Mobilfunk-Karte aktiviert werden. Patiño forderte die britische Regierung auf, die Untersuchung zu unterstützen. Er verdächtigte das in England ansässige Sicherheitsunternehmen Surveillance Group Limited, die Wanze installiert zu haben. Die Firma wies den Vorwurf zurück.

Patiño meinte, die Aktion habe offensichtlich nichts mit dem flüchtigen früheren US-Geheimdienstmitarbeiter Edward Snowden zu tun. In Ecuadors Londoner Botschaft harrt der Australier Assange seit rund einem Jahr aus, um einer Auslieferung nach Schweden zu entgehen. Die ihm dort zur Last gelegten Sexualdelikte nennt der 41-Jährige vorgeschoben. Er fürchtet, an die USA ausgeliefert zu werden. Dort droht Assange wegen Geheimnisverrats eine lebenslange Haftstrafe. Assange hält sich jedoch in einem anderen Teil des Gebäudes auf als dem, wo die Wanze gefunden wurde.

Kurz zuvor war über die Presse berichtet worden, dass der US-Geheim-

dienst NSA gezielt Einrichtungen der Europäischen Union ausgespäht hat, was sich aus geheimen Dokumenten ergibt, die der frühere Geheimdienst-Mitarbeiter Edward Snowden mitgenommen habe. Der Geheimdienst soll Wanzen im Gebäude der EU-Vertretung in Washington installiert und auch das interne Computernetz infiltriert haben. Auf die gleiche Art und Weise sei auch die EU-Vertretung bei den Vereinten Nationen attackiert worden (Wanze in Ecuadors Botschaft, SZ 05.07.2013, 7; Ecuador beklagt Lauschangriff, www.n-tv.de 03.07.2013).

### Großbritannien

## Barclays-Bank wird Kundendaten verkaufen

Die britische Großbank Barclays will die Daten ihrer KundInnen nutzen und Fotos, Stimmaufzeichnungen und Facebook-Kommentare kommerziell verwerten. Auch die Politik soll von den Daten profitieren. Nach Presseberichten soll von Herbst 2013 an das Wissen der Bank über die Ausgabegewohnheiten ihrer KundInnen an Dritte weiterverkauft werden. Die Daten sollen auch an Ministerien und Parlamentsmitglieder weitergegeben werden können, die dadurch mehr über die Interessen in ihrem Wahlkreis erfahren könnten. Mehr als 13 Millionen Kontoinhabende sollen davon betroffen sein. Barclays informierte sie in einem Brief über die geplanten Änderungen. Zu den betroffenen Daten gehören danach „Fotos und Stimmaufnahmen“ der Kunden sowie Kommentare in sozialen Medien wie Facebook und Twitter, die bei einer Interaktion mit der Bank gemacht wurden. Die gesammelten Informationen sollen zusammengefasst werden, um Trends zu zeigen. Individuen sollen dabei nicht identifizierbar sein. In dem Brief teilte das Geldhaus Barclays auch mit, dass es Mobiltelefon-Daten sammeln möchte, die Aufschluss darüber geben, wo sich der Kunde befindet. Allerdings soll das nur dann passieren, wenn ein Betrug vermutet wird. Die Daten über den Aufenthaltsort könnten dann mit dem Ort der verdächtigen Transaktion abgeglichen werden (Barclays verkauft Kundendaten, SZ 26.06.2013, 25).

### Litauen/Estland

## Steuerfahndung mit Hilfe von Google Street View

Die beiden baltischen Länder Litauen und Estland wird zum Aufspüren von Steuerhinterziehern der Internet-Panoramadienst Google Street View eingesetzt. Dazu vergleicht man Behördendaten mit den von Google gemachten Fotos und forscht nach, wenn man Häuser und Baustellen findet, die dort eigentlich gar nicht sein sollten. In Litauen wurden die Finanzbehörden nach Angaben ihres Sprechers Darius Buta so auf etwa 100 Hausbesitzer und 30 Firmen aufmerksam, gegen die nun ermittelt wird. Die litauischen Steuerfahnder ermitteln so im warmen Büro, statt sich im Außendienst Wind und Wetter auszusetzen.

Google Street View ist nicht das einzige neuere und allgemein verfügbare technische Angebot, das von Behörden zur Steuerfahndung eingesetzt wird: In Griechenland nutzt man Satellitenbilder, in den USA gleicht die Bundessteuerbehörde Internal Revenue Service (IRS) Angaben aus Steuererklärungen mit solchen aus Facebook und Twitter ab, in Großbritannien sucht eine Software automatisch nach nicht deklarierten Verkäufen bei Online-Auktionshäusern. Durch die Verknüpfung sehr vieler Daten können dabei auch aus scheinbar trivialen Informationen Hinweise auf ein ungewöhnliches und möglicherweise rechtswidriges Verhalten gewonnen werden. Allerdings ist das Risiko groß, dass mit solchen Methoden auch Unschuldige ins Visier der Behörden geraten (Litauen und Estland suchen Steuerhinterzieher mit Google Street View, www.heise.de 21.04.2013).

### Schweden

## Memoto entwickelt Life-Log-Kamera

Die schwedische Firma Memoto in Stockholm, ein 2012 gegründetes Start-up mit 17 festen Mitarbeitenden aus Schweden, Singapur und den USA, entwickelt eine Minikamera mit Datenspeicherung, welches als Gedächtnis der Nutzenden dienen und den Blick auf diese verändern soll. Die Kamera ist so winzig wie eine Streichholzschachtel. Die Memoto-Kamera kann mit einem Clip an der Kleidung befestigt oder an einer Kette um den Hals getragen werden. Sie macht automatisch alle 30 Sekunden ein Bild, 120 Bilder pro Stunde, 2880 am Tag. Zu jedem Bild speichert das Gerät die Uhrzeit und per GPS den Ort, womit ein riesiges Fototagebuch erstellt wird, ein „Life Log“. Die Bilder werden auf den Servern von Amazon übertragen, das diese für Memoto speichert. Die Memoto-Software sortiert die Fotos, ordnet sie nach Motiven und Zeiten und markiert die technisch gelungensten. Der oder die Nutzende kann die Bilder über ein Smartphone abrufen, weiter bearbeiten oder z. B. über Facebook posten. Die Memoto-Kamera ist immer aktiv; sie lässt sich nur dadurch stoppen, dass sie in die Tasche gesteckt wird.

Martin Källström, Gründer von Memoto ist nicht der erste, der Life Logs entwickelt. Der kanadische Erfinder Steve Mann oder der Microsoft-Manager Gordon Bell experimentierten schon viele Jahre früher mit Geräten, die ihre Sinneseindrücke möglichst für immer bewahren sollten. Memoto will daraus ein Massengeschäft machen – sozusagen die totale Erinnerung für Jedermann. Ein bisschen appelliert Källström, die Privatsphäre anderer zu achten: „Respektiert, dass andere Menschen manchmal nicht fotografiert werden möchten“. Doch das sei „Sache der Nutzer“. Memoto habe keinen Zugriff auf die Daten, ebenso wenig die Werbeindustrie. Das Geld soll durch den Verkauf der Kameras verdient werden. Für 279 Dollars kann ein Exemplar reserviert werden; Auslieferung noch im Jahr 2013. Einer der Vorbilder ist für Memoto Instagram, das auch mit zwölf Mitarbeitenden anfing und 2012 von Facebook für eine Milliarde Dollar übernommen wurde. Instagram änderte danach für einige Monate vorübergehend seine Geschäftsbedingungen und lies sich umfassende Nutzungs- und Verwertungsrechte an den Fotos

der Nutzenden einräumen (Wolf, Totale Erinnerung, Der Spiegel 18/2013, 111).

### Tschechien

## Bürochefin vom Premier lässt dessen Ehefrau bespitzeln

Tschechische Polizeiermittler gaben am 14.06.2013 bekannt, dass die wegen einer Korruptionsaffäre festgenommene Kabinettschefin des tschechischen Premierministers Petr Necas, Jana Nagyova, beim Heeresnachrichtendienst (VZ) die Bespitzelung von drei Privatpersonen bestellt habe. Bei einer der bespitzelten Personen soll es sich um die Ehefrau von Necas, Radka Necasova handeln. Medien und Politiker behaupten schon seit Längerem, dass das Verhältnis zwischen Necas und Nagyova „über die Arbeitssphäre hinausgeht". Nagyova leitete das Sekretariat von Necas seit 2006, als dieser noch Arbeitsminister war. Ihr wird ein „starker Einfluss" auf den Premier nachgesagt. Necas hatte angekündigt, dass er sich von seiner Ehefrau scheiden lasse. Die Ermittler bezeichneten die Motive der Bespitzelung als „rein privat". Es sei wohl darum gegangen, Beweise für die eheliche Untreue der Gattin zu finden und Necas zur Scheidung zu drängen. Ob Necas von der Bespitzelungsanordnung seitens Nagyovas gewusst hat, ist nicht bekannt. Er erklärte, dass er den Übergriff „zutiefst bedauert" und missbilligt. Necas hatte Nagyova bis zum Schluss verteidigt, obwohl er offenbar zumindest ahnte, dass sie ein böses Spiel hinter seinem Rücken gespielt hat. Am 17.06.2013 erklärte Necas, dass er zurücktreten werde.

Die Bespitzelungsaktion steht in Zusammenhang mit der Aufdeckung einer Korruptionsaffäre, bei der Necas abweichlerische Abgeordnete zur Niederlegung ihres Parlamentsmandats gegen lukrative Posten bei Staatsfirmen veranlasst haben soll. Bei einer Razzia sind nach Ermittlungsangaben acht Personen festgenommen, sowie etwa 150 Millionen Kronen (5,83 Millionen Euro) in bar und dutzende Kilogramm Gold beschlagnahmt worden. Die Affäre sorgte für einen Schlagabtausch im Parlament. Die oppositionellen Sozialdemokraten (CSSD) hatten den sofortigen Rücktritt von Necas und seiner gesamten Regierung sowie baldige Neuwahlen gefordert, so CSSD-Chef Bohuslav Sobotka im Abgeordnetenhaus: „Noch nie in der Geschichte des Landes hat die Polizei in das Regierungsamt eingegriffen." Necas' Kabinett sei „total diskreditiert". Necas hatte zunächst die Rücktrittsforderungen zurückgewiesen und das Vorgehen der Polizei und der zuständigen Staatsanwaltschaft scharf kritisiert. Bei der Polizeirazzia und den von der Polizei erhobenen Vorwürfen handele es sich um ein „medial-politisches Gulasch mit brisantem Inhalt", in dem mehrere Sachen vermischt worden seien, die überhaupt nicht miteinander zusammenhingen (Brill, Tschechischer Premierminister zwischen zwei Frauen, SZ 17.06.2013, 4; Schmidt, Necas stürzt über Liebe zu korrupter Büroleiterin, www.welt.de 17.06.2013; Necas' Sekretärin soll Premiers-Ehefrau bespitzelt haben; www.wienerzeitung.at, 14.06.2013).

### Ungarn

## Sicherheitsüberprüfungen ohne rechtsstaatliche Kontrolle

Nachdem sich das ungarische Parlament auf ein verändertes Gesetz zum „Schutz der Heimat" geeinigt hat, befürchtet die Kommission der Europäischen Union (EU) in Brüssel, dass damit vor allem RichterInnen und StaatsanwältInnen rechtsstaatswidrig ausspioniert und damit unter Druck gesetzt werden könnten. Das Gesetz regelt die Sicherheitsüberprüfung für Beamte, aber auch für PolitikerInnen, die Zugang zu vertraulichen Unterlagen haben. In einem Brief an das ungarische Parlament hatte der stellvertretende ungarische Generalstaatsanwalt Andras Varga Ende Mai 2013 gegen das Gesetz als „eine Quelle für den Missbrauch der politischen Macht" protestiert, die gegen die ungarische Verfassung verstoße. Vor dem Ausschuss des Europäischen Parlamentes für Bürgerliche Freiheiten, Justiz und Inneres forderte der portugiesische Europaabgeordnete Rui Tavares am 06.06.2013 darum von der ungarischen Regierung eine „offizielle Übersetzung" des gerade verabschiedeten Gesetzes, um es auf seine Vereinbarkeit mit den europäischen Werten prüfen zu können.

Gegen die Regierung von Ministerpräsident Orbán, dessen Partei Fidesz mit einer Zweidrittelmehrheit regiert, hatte die EU-Kommission schon einmal ein Verfahren eröffnet, weil die ungarischen RichterInnen und StaatsanwältInnen unter Druck gesetzt werden sollten. Die Kritik an dem nun vorliegenden Heimatschutzgesetz richtet sich vor allem dagegen, dass die Regierung eine Überprüfung mit geheimdienstlichen Mitteln für bis zu 60 Tage pro Jahr anordnen kann, ohne ein Gericht fragen zu müssen. Auch hätten die Betroffenen keine Klagemöglichkeit, wenn sie aufgrund der Erkenntnisse entlassen oder gar nicht erst eingestellt werden, wenn sie sich für den Justizdienst bewerben. Diese Art der staatlichen Überprüfung trifft auch sonstige BeamtInnen, die mit vertraulichen Vorgängen zu tun haben könnten. Dabei werden einfache GeheimnisträgerInnen (Stufe „vertraulich") genauso behandelt, wie die der höchsten Stufe („streng geheim"). Bei der Überprüfung darf der Nationale Sicherheitsdienst, der unter der Verantwortung des Innenministeriums steht, Telefone abhören, Privatwohnungen per Video überwachen und Post öffnen. Vize-Generalstaatsanwalt Andras Varga kritisiert in seinem Brief an Barroso auch, dass Kriterien wie eheliche Treue, Verhalten außerhalb der Arbeit oder finanzielle Verhältnisse inspiziert werden sollen. Mit solch weit gefassten Kriterien bei der Sicherheitsüberprüfung könnte die Regierung selbst dann Kündigungen aussprechen, wenn der Betroffene sich rechtlich einwandfrei verhalten hat (Winter, Big Brother in Budapest, SZ 08./09.06.2013, 9).

### Russland

## Verkehrsministerium will Fluggastdaten von europäischen Fluggesellschaften

Fluggesellschaften sollen künftig persönliche Daten von Russlandreisenden an die russischen Behörden übermitteln. Nach Presseberichten sieht ein Dekret

des russischen Verkehrsministeriums vor, dass Airlines, die russisches Gebiet überfliegen oder dort landen oder starten wollen, ab 1. Juli 2013 den Behörden in Moskau sämtliche Daten übermitteln, die bei der Buchung von Flugtickets anfallen, also z. B. Nummern von Kreditkarten, Sitzplatzpräferenzen, aber auch Adressen und Kontaktdaten am Zielort in Russland. Das Dekret unterscheidet nicht zwischen Flugreisenden und Passagieren von Schiffen, Zügen oder Bussen. Der Streit belastet das bevorstehende Gipfeltreffen der Europäischen Union (EU) und Russlands in Jekaterinburg. Der Sprecher von EU-Innenkommissarin Cecilia Malmström zeigte sich „äußerst besorgt". Sollte Moskau nicht einlenken, gerieten europäische Fluggesellschaften in einen Konflikt zwischen Normen der EU und der Russischen Föderation. In letzter Konsequenz droht, so die Vermutung, das Verbot, russische Flughäfen und russischen Luftraum zu nutzen.

Fluggesellschaften dürfen nach EU-Recht persönliche Daten ihrer Passagiere nicht ohne weiteres an Drittstaaten weitergeben. Denkbar wäre das nur auf der Basis eines Datenschutzabkommens, wie es beispielsweise 2012 die EU und die USA über Fluggastdaten geschlossen haben. Damals hatte es heftige Diskussionen über den Datenschutz gegeben. Auch innerhalb der EU gibt es Pläne für die Sammlung von Passagierdaten. Die Fluggesellschaften sollen dabei verpflichtet werden, die Daten, die sie bei der Buchung abfragen, an Registerstellen in der EU zu melden. Ein erster Anlauf für eine Richtlinie war jedoch Ende April im EU-Parlament gescheitert.

Der Europaabgeordnete Knut Fleckenstein (SPD) erklärte, er sei von besorgten und ratlosen Vertretern diverser Airlines aufgesucht worden. Malmströms Sprecher zufolge gestaltet sich die Kommunikation mit Russland zäh. Die Kommission sei nicht vorab informiert worden, ein Brief vom 15.03.2013 sei unbeantwortet geblieben. In Brüssel wird vermutet, dass Russland seine Forderung wie die USA mit der Abwehr von Terrorismus und Schwerverbrechen begründen wird. Moskau wolle von der EU nicht anders behandelt werden als die USA. Fleckenstein sagte, die russischen Ansprüche auf Fluggastdaten seien im Rahmen der lange stockenden Verhandlungen über Visums-Erleichterungen aufgekommen. Wenn die Russen „nun auf der Schlussgeraden dieser Verhandlungen einen ganzen Baumstamm in den Weg legen", stelle sich die Frage, wie groß das Interesse an einer Einigung sei. Die Kommission könne hier keine Zugeständnisse machen. Er forderte Moskau auf, das Dekret vorübergehend aufzuheben, um den Weg für Verhandlungen über ein Datenschutzabkommen zu ebnen. EU-Diplomaten zufolge dürfte über ein solches Moratorium gesprochen werden. Derweil gibt es weitere Länder mit Begehrlichkeiten. Der Grünen-Europaabgeordnete Jan-Philipp Albrecht bestätigte, dass auch Katar und Saudi-Arabien Fluggastdaten haben wollen (Cáceres, Russland will Fluggastdaten aus EU-Ländern, SZ 03.06.2013, 1, 4; Russland verlangt Fluggastdaten aus EU-Ländern, www.spiegel.de 03.06.2013).

### Russland

## Sicherheitsdienste nutzen analoge Technik

Russische Geheim- und Sicherheitsdienste nutzen zum Schutz vor digitaler Spionage Schreibmaschinen. Der Föderale Schutzdienst (FSO), der für die Sicherheit des Präsidenten und der Regierung zuständig ist, bestellte nach Berichten russischer Medien 20 Schreibmaschinen. Für die Sicherheitsdienste sei wichtig, dass jede Schreibmaschine ihre eigene Signatur habe – anders als etwa in Serienproduktion hergestellte Drucker. So könne jedes Dokument einer bestimmten Maschine zugeordnet werden. Das deutsche Modell Triumph-Adler Twen 180 sei bei den russischen Geheimdiensten besonders beliebt. Der frühere Chef des Inlandsgeheimdienstes FSB, Nikolai Kowaljow, bestätigte, auch die handschriftliche Aufzeichnung geheimer Informationen sei üblich. Besonders heikle Dokumente würden nur auf Papier und nicht auf elektronischen Datenträgern archiviert, um sie zu schützen. Üblich sei diese Praxis in Russland nicht nur bei den Geheimdiensten, sondern auch im Verteidigungs- und im Zivilschutzministerium. Der Sprecher des russischen Staatsschutzes FSO, Sergej Dewjatow, erklärte, auch alte abhörsichere Telefonleitungen würden weiter für vertrauliche Gespräche zwischen den Staatsführungen genutzt. Die erste Leitung zwischen der Sowjetunion und den USA sei vor gut 50 Jahren am 20.06.1963 eingerichtet worden (Russische Geheimdienste kramen die Schreibmaschine raus, www.zeit.de 11.07.2013).

### Iran

## Digitale Abschottung zwecks Überwachung der Bevölkerung

Der iranische Informations- und Kommunikationsminister Mohammed Hasan Nami ließ über das Staatsfernsehen verkünden, sein Land habe einen eigenen E-Mail-Dienst gestartet. Bis 2015 will sich Iran laut Plan schrittweise vom weltweiten Datennetz abkoppeln und sein eigenes Internet schaffen – das nationale Intranet „Halal Internet", um die staatliche Kommunikationsüberwachung zu erleichtern. Beim neuen Mail-Dienst, der von der staatlichen Post betrieben wird, soll jede BürgerIn des Landes eine Kontaktadresse zugewiesen bekommen. Entwickelt worden sei die Software dem Minister zufolge von „Experten vor Ort".

Auf dem Weg zum nationalen Netz kommt Iran voran. VPN-Verbindungen ins Ausland werden staatlich kontrolliert. Populäre soziale Netzwerke wie Facebook oder Twitter sind für die Bevölkerung gesperrt, ebenso Gmail, der E-Mail-Dienst von Google. Stattdessen entwickelt Iran eigene Alternativen, um die Sperrung ausländischer Webseiten auszugleichen. Zuvor hatte Iran etwa einen staatlichen Video-Dienst vorgestellt. Das Regime soll auch an einem Google-Earth-Klon arbeiten. In Iran gibt es laut offiziellen Informationen etwa 32 Millionen Internetnutzer. Nach den Präsidentschaftswahlen 2009 war es in dem Land zu Massenprotesten gegen die Führung des Landes gekommen. Die Proteste wurden damals unter anderem

über das Internet organisiert (Iran startet eigenes E-Mail-System, www.sueddeutsche.de 08.07.2013).

USA

## Regierung auf Jagd gegen Enthüllungsjournalisten

Nach der Vertuschungsaffäre um den Terroranschlag auf das US-Konsulat in Bengasi und den Strafaktionen der Steuerbehörde IRS gegen Tea-Party-Gruppen und vor den Enthüllungen zum Spähprogramm der National Security Agency (NSA) Prism wurde bekannt, wie die US-Regierung unter Präsident Barack Obama, dem seit jeher unterstellt wird, ein gespaltenes Verhältnis zu den Medien zu haben, diese ausspähen ließ. Im Rahmen des Versuchs der US-Regierung, Geheimnisverräter aus den eigenen Reihen zu überführen, hat diese die Agentur Associated Press (AP) ausgespäht. In einem offenen Brief an US-Justizminister Eric Holder protestierte der AP-Präsident Gary Pruitt am 13.05.2013 „auf schärfste Weise“ gegen den „massiven und beispiellosen Eingriff“ in die Arbeit seiner Reporter. Dafür gebe es „keine denkbare Rechtfertigung“. Das Schreiben endet mit den spitzen Worten: „Ich freue mich auf Ihre baldige Antwort.“ Das Justizministerium habe sich heimlich die Verbindungsdaten von mehr als 20 Telefonnummern der Agentur und seiner JournalistInnen beschafft. Es handele sich dabei um Anruflisten von April und Mai 2012. Betroffen sind mehr als hundert JournalistInnen, dienstliche wie private Anschlüsse, eine zentrale Fax-Nummer – sowie das AP-Telefon in der Pressegalerie des US-Kongresses, das auch viele andere Reporter nutzen. Das Ministerium kann damit einsehen, wer wen wann anrief und so die Quellen der Agentur aufdecken – auch die anonymen.

Am 07.05.2012 hatte AP eine CIA-Operation im Jemen enthüllt, die einen Qaida-Anschlag vereitelt habe. Diese Meldung widersprach der Lesart des Weißen Hauses, das nach außen hin versichert hatte, es habe „keine glaubhaften Informationen“ über Terrorpläne gegeben. Monatelang hatte danach die Regierung versucht herauszufinden, woher AP das wusste. Sogar CIA-Direktor John Brennan wurde vom FBI befragt. Der dementierte, die Quelle gewesen zu sein, und verurteilte die Veröffentlichung als „unautorisiert und gefährlich“. Denn später stellte sich heraus, dass der angebliche Attentäter ein US-Spion war, der den jemenitischen al-Qaida-Arm infiltriert hatte. Der AP-Bericht habe, so Minister Holder, „Amerikaner in Gefahr gebracht“. Er kündigte im Juni 2012 zwei „Sonder-Ermittlungen“ zu den Lecks an; die eine galt dem Vorfall im Jemen, die andere einem Leak zum Iran. David Sanger von der New York Times hatte berichtet, wie die USA im Cyberkrieg gegen Iran per Stuxnet-Wurm Teherans Computer und Uran-Zentrifugen aus dem Gleichgewicht brachten. Damals kritisierten die Republikaner, Holder tue zu wenig, um die undichten Stellen zu finden und die redseligen Beamten zu bestrafen. Die beteiligten AP-Reporter gehörten zu den Betroffenen, deren Telefondaten die Justiz einkassierte. Hinweise, dass Gespräche abgehört oder mitgeschnitten wurden, gibt es nicht. Der zuständige Staatsanwalt Ronald Machen ließ erklären, er habe sich bei den Ermittlungen um einen Ausgleich bemüht zwischen dem öffentlichen Interesse an freier Berichterstattung einerseits und ordentlicher Rechtspflege andererseits.

Die indirekte Enttarnung von InformantInnen entsetzte die Medienwelt, deren Enthüllungen staatlicher Missstände vom Schutz diskreter Quellen abhängen. AP ist ein Konsortium der gesamten US-Presse, mit mehr als 1700 Tageszeitungen und rund 5000 Hörfunk- und Fernsehsendern. Der Watergate-Enthüller Carl Bernstein meinte, diese Form von „Einschüchterung“ sei „völlig unverzeihlich“. Die langjährige Washington-Korrespondentin Andrea Mitchell sprach von „einem der empörendsten“ Akte, „die ich in meiner Zeit hier erlebt habe“. John Cassidy, Reporter des „New Yorker“, erinnerte an George Orwells diktatorisches Spitzelsystem „Big Brother“: „Was haben sie sich nur gedacht?“

Obamas Sprecher Jay Carney erklärte am 14.05.2013, das Weiße Haus wisse von nichts. Der Präsident sei auf jeden Fall „ein felsenfester Verfechter“ der Pressefreiheit – aber nur, solange das keine sicherheitsrelevanten Informationen betreffe. Kurz darauf trat Holder schwitzend vor die Presse. Er selbst habe keine direkte Kenntnis von dem AP-Fall, der von seinem Vize James Cole gehandhabt werde. Aber er sei sicher, dass alles vorschriftsgemäß abgelaufen sei. Holder erklärte nach Bekanntwerden der Spitzelaktion, er wolle die hauseigenen Richtlinien „aktualisieren“. Er suchte das Gespräch mit den Journalistinnen und wärmte eine alte Idee auf, mit einem „Presseschutz-Gesetz“ Journalistinnen mehr Rechte gegenüber eifrigen StaatsanwältInnen zu gewähren. Doch auch dieser Gesetzentwurf sieht so viele Ausnahmen vor, dass das FBI weitermachen könnte wie bisher.

Obama predigt gerne Transparenz, geht aber seit jeher knallhart gegen GeheimnisverräterInnen in den eigenen Reihen vor – und gegen die ReporterInnen, denen sie ihre Interna stecken. Zwar lanciert das Weiße Haus selbst immer wieder Top-Secret-Informationen, um sich in ein gutes Licht zu setzen – etwa die Details über den Tod von al-Qaida-Chef Osama Bin Laden. Doch wer auf eigene Faust aus dem Nähkästchen plaudert, wird gnadenlos verfolgt. Sechs „Whistleblower“ hat Obama bisher vor die Gerichte bringen lassen, doppelt so viele wie unter allen US-Präsidenten zuvor. Die Obama-Administration beantwortet erheblich weniger Anfragen nach dem US-Informationsfreiheitsgesetz (Freedom of Information Act) als die Regierung von George W. Bush. Um Beamte besser überwachen zu können, versucht die Regierung, alle Staatsbedienstete, selbst Ranger in Nationalparks oder Mitarbeitende in Katasterämtern, pauschal als „mit nationaler Sicherheit befasst“ einzustufen. Der konservative Politologe Gabriel Schoenfeld schreibt in seinem Buch „Necessary Secrets“: „Ironischerweise verantwortet Obama das härteste Durchgreifen gegen Leaks in unserer Geschichte. Mehr noch als Nixon“. (Pitzke, US-Medien entsetzt über staatliche Spitzelei, www.spiegel.de 14.05.2013; Wernicke, Big Brother kehrt zurück, SZ 15.05.2013, 5; Richter,

Überzogener Ermittlungseifer, SZ 15.05.2013; Schmitz, Der Serientäter, Der Spiegel 21/2013, 134f.; Wernicke, Ein Hauch von Nixon, SZ 31.05.2013, 47).

USA

## Verdacht gegen IRS wegen tendenziöser Ermittlungen

Im April 2010 begannen BeamtInnen des Internal Revenue Services (IRS), der von vielen verhassten und von rechtskonservativen BürgerInnen als „illegal" geschmähten US-Bundes-Steuerbehörde, damit, Anträge auf Steuerbefreiung von gesellschaftlich aktiven Gruppen nach Gesinnung zu sortieren. Wer Begriffe wie „Tea Party" oder „Patrioten" im Namen trug, sah sich langen Prüfungen und umfangreichen Nachfragen ausgesetzt. Die Obama-GegnerInnen sollten ihre SpenderInnen offenlegen, genauestens Rechenschaft über ihre Aktivitäten ablegen und Presseartikel über sich herbeischaffen. Linke Gruppen blieben währenddessen verschont.

US-Präsident Barack Obama versicherte, das Weiße Haus habe bis zum 10.05.2013 von dieser Polit-Willkür nichts gewusst. Die anfängliche Behauptung, kleine IRS-Bürokraten in einer Außenstelle in Cincinnati hätten „Fehler begangen", erwies sich als unzutreffend. Die BeamtInnen bestimmten vielmehr die Prüfregeln für die gesamte Nation und selbst nach einem mahnenden Eingriff einer Vorgesetzten im Sommer 2011 wurde die Diskriminierung fortgeführt. Statt am bloßen Namen orientierte sich die IRS nun an der Mission der Politgruppen. Wer „eine Begrenzung/Ausweitung der Regierung" anstrebe, wer „über die Verfassung oder die Bill of Rights belehrt" – Kernmissionen der Tea Party – bekam es mit den SteuerprüferInnen zu tun. Gemäß Presseberichten sollen IRS-BeamtInnen in Washington D.C. einer rechten Gruppe aus Texas im Gespräch offen gestanden haben, sie würden „nur das tun, was Washington sagt" (Wernicke, Big Brother kehrt zurück, SZ 15.05.2013, 5).

USA

## Supreme Court akzeptiert routinemäßige DNA-Identifikation

Das höchste Gericht in den USA, der Supreme Court, entschied im Fall „King" mit einer knappen Mehrheit von 5 der 9 Richter, dass ein Staat nicht exzessiv handelt, wenn er sich den DNA-„Fingerabdruck" sämtlicher Personen per Wattestäbchen aus der Mundhöhle erhebt und speichert, wenn ein Straftatverdacht vorliegt. Hierfür benötigt die Polizei keinen richterlichen Beschluss. Es bedarf auch keiner Verdächtigung bestimmter Taten, etwa Sexualstraftaten. Hintergrund der Entscheidung war eine DNA-Entnahme bei einem Verdächtigen eines einfachen Raubüberfalls im Jahr 2009 durch die Polizei in Maryland. Beim Vergleich in der DNA-Datenbank stellte die Polizei fest, dass die DNA zu einem ungelösten Fall, einer Vergewaltigung im Jahr 2003, passte. Die pauschale Entnahme von DNA-Proben ist in 28 der 50 US-Staaten gängig. Im Fall King hatte ein Berufungsgericht noch entschieden, dass es gegen die Grundrechte verstößt, wenn die DNA eines jeden Verdächtigen überprüft wird, noch bevor die Justiz überhaupt Schuld oder Unschuld festgestellt hat.

Diese Entscheidung wurde nun aufgehoben. Aus Sicht der Mehrheit des Gerichts wurde nicht darauf abgestellt, dass es um die Klärung von Altfällen gehe. Vielmehr wurde die Maßnahme einfach als ordentliche Identifizierungsmaßnahme legitimiert, so Richter Anthony Kennedy: „Der DNA-Abstrich ist, wie Fingerabdrücke oder Fotos, eine legitime erkennungsdienstliche Maßnahme." Zwischen DNA- und normalem Fingerabdruck bestehe also kein rechtlicher Unterschied.

Die unterlegene Minderheit im Gericht widersprach mit seltener Heftigkeit. Richter Antonin Scalia meinte, das Urteil strapaziere die „Leichtgläubigkeit der Leichtgläubigen". Es verkenne, wozu die Routine-DNA-Tests heute wirklich dienten, nämlich zum Lösen der „cold cases", also von Altfällen: „Täuschen Sie sich nicht: Wegen der heutigen Entscheidung kann Ihre DNA entnommen und in einer landesweiten Datenbank gespeichert werden, wenn Sie auch nur einmal festgenommen werden, zu Recht oder zu Unrecht, warum auch immer." Nach Ansicht der Minderheit verstößt dies gegen den 4. Zusatz zur US-Verfassung, der verhindern soll, dass der Staat ohne Anlass oder Verdacht in die Privatsphäre seiner Bürger eindringt. Gerade der Fall King zeige, dass das Urteil falsch ist: King sei auch ohne DNA identifiziert worden, die Polizei habe Namen, Rasse, Geschlecht, Größe, Gewicht, Geburtsdatum und Adresse gekannt. Scalia erinnerte an die Revolutionäre, die einst die Verfassung prägten: „Diese stolzen Männer hätten nicht so bereitwillig ihren Mund geöffnet für königliche Kontrollen". (Richter, Wattestäbchen auf Verdacht, SZ 05.06.2013, 1).

USA

## Postdienst erfasst gesamten Inlandsbriefverkehr

Gemäß Presseberichten werden in den USA im eigenen Land gewöhnliche Postsendungen vollständig vom staatliche Postdienst US Postal Service (USPS) abfotografiert. Von dem Überwachungsprogramm „Mail Isolation Control and Tracking" (MICT) seien im Jahr 2012 rund 160 Milliarden Briefe betroffen gewesen. Absender und Empfänger von jeder Sendung, die über den staatlichen Postdienst USPS verschickt wird, würden elektronisch erfasst. Für den Zugang genüge ein schriftlicher Antrag, den die Post im Normalfall nicht ablehnt. Die „New York Times" beruft sich bei diesem Bericht u. a. auf Mitarbeiter des US-Justizministeriums und einen ehemaligen Agenten der amerikanischen Bundespolizei FBI. Das Programm diene vor allem der Arbeit von amerikanischen Strafverfolgungsbehörden. Die Sendungen würden nicht geöffnet. Gemäß einer mehr als 100 Jahre alten Vorgehensweise würden Daten wie Absender, Empfänger oder Einwurfsort registriert und vor Auslieferung der Sendung an Sicherheitsbehörden weiter-

gegeben. Diese Routine-Überwachung wurde nach dem 11.09.2001 nach Attentaten mit vergifteten Anthrax-Briefen, die fünf Menschenleben forderten, intensiviert. Wie lange die Behörden die gesammelten Daten speichern, sei noch unklar (US-Regierung überwacht gesamten Briefverkehr in USA, www.focus.de 04.07.2013; Havererz, Mal eben den Empfänger scannen, www.taz.de 04.07.2013; Richter, Verbogene Wahrheiten, SZ 05.07.2013, 8).

USA

## Google will „Policy Violation Checker“ patentieren

Google hat ein Patent auf sein Tool „Policy Violation Checker“ beantragt, eine Software, die elektronische Texte, z. B. Mailinhalte, auf politische Korrektheit hin überprüft und bewertet. Das Tool funktioniert nach dem Prinzip der Auto-Korrektur und erkennt schon während des Tippens Wortfolgen und Sätze, die nicht gestattet sind. Was genau verboten ist, kann individuell programmiert werden – vom Staat, einem Unternehmen oder einer Privatperson. Wo die Software eingesetzt werden soll, ist bisher nicht klar; möglich ist aber vieles. Der „Policy Violation Checker“ soll so programmiert sein, dass er auffällige Mails direkt an Dritte weiterleiten kann, also beispielsweise an die Rechtsabteilung der Firma, den Chef oder die Polizei. Das Programm kann den Schreiber warnen und darüber informieren, worin der Policy-Verstoß liegt oder korrekte Alternativformulierungen vorschlagen. Google preist sein Patent als ein Instrument an, mit dem Unternehmen vor Gerichtsverfahren wegen diskriminierenden, beleidigenden oder geschäftsschädigenden Veröffentlichungen bewahrt werden können.

Viele Blogger reagierten empört, so z. B. TechWeek: „Damit hat sich Google endgültig den Big Brother-Stempel aufgedrückt.“ Die Huffington Post fragte: „Wird man als Mörder verurteilt, wenn man seinen Mitbewohner ‚umbringt‘, weil er die Küche nicht geputzt hat?“ Es wird darüber spekuliert, wie der Policy Checker in Unternehmen eingesetzt werden könnte oder wie Regierungen, eventuell in Diktaturen, damit die Bevölkerung überwachen könnten. Der amerikanische Blog Rough Type schreibt, dass Google „böse Gedanken“ am liebsten schon dort auslöschen würde, wo sie entstehen. Sergey Brin, der Entwickler der Suchmaschine, witzelt im Buch „The Google Story“, dass ein kleiner Google-Adapter irgendwann unsere Gehirne verbessern könnte. Nicht das, was man denkt, aber immerhin alles, was man schreibt, kann derart ausgewertet werden. Google entwickelte also ein Werkzeug, mit dem Gehirnwäsche und Gedankenpolizei praktiziert werden können. Ob Google das Patent zum Policy Violation Checker anerkannt erhält, ist noch nicht klar. Durch den Protest im Netz hat das Unternehmen zunächst öffentlich zurück gerudert. Der Antrag auf das Patent läuft aber weiter. Slashdot berichtete als Erster über den Patentantrag und appellierte – in Anspielung auf das Unternehmensmotto: „Tu nichts Böses“ (do no evil): „Wenn Du schon nicht Nichts Böses tun kannst, so könntest Du zumindest nichts Böses aufdecken!“

Dass Googlemail Nachrichten auf Inhalte untersucht, ist nichts Neues. Es ist normal, dass der Browser Werbung für eine Last-Minute-Reise in der Algarve zeigt, nachdem man mit einer Freundin über den Surftrip in Portugal gemailt hat. Die aktuelle Software würde jedoch einen Schritt weitergehen. Ob Google die Software auf Googlemail anwenden wird, ist unklar.

In Deutschland gilt das Recht auf Brief- bzw. Telekommunikationsgeheimnis, das auch auf E-Mails anzuwenden ist. Alles, was zwischen zwei Personen geschrieben wird, darf grundsätzlich von niemand anderem gelesen werden. Nur in Ausnahmefällen darf die Polizei Inhalte zur Strafverfolgung nutzen. Ein entsprechender Einsatz der geplanten Google-Software würde gegen das europäische Telekommunikations- und Fernmeldegeheimnis verstoßen. Es ist aber noch eine ganz andere Qualität, ob man eine Auswertung von Begriffen macht, um Werbung zu schalten oder ob Meinungsinhalte ausgewertet werden, um hiervor zu warnen oder direkt zu intervenieren. Da eine inhaltliche Bewertung erfolgt, wäre der Einsatz in Europa zudem als Eingriff in das Grundrecht auf Meinungsäußerungsfreiheit einzustufen. Das Ansinnen Googles, politische Korrektheit zu kontrollieren, nimmt nicht nur Einfluss auf den jeweiligen User, sondern auf die gesamte Gesellschaft (Google Aims To Patent Policy Violation Checker, Potentially Revolutionizing Email Snooping, www.huffingtonpost.com 06.05.2013; Bühler, Googles neues Spionage-Tool, www.br.de 10.05.2013).

# Technik-Nachrichten

## Snapchat: Digitaler Bilderselbstzerstörungsdienst

Als Evan Spiegel (22) an der Eliteuniversität Stanford in seiner Abschluss-Arbeit die Entwicklung einer mobilen App präsentierte, mit der Freunde Fotos teilen können, die nach dem Ansehen automatisch gelöscht werden, erntete er zunächst wenig Resonanz. Als Spiegel und sein Partner Bobby Murphy (24) aber im September 2011 eine erste Version im Internet anboten, landeten sie einen Treffer. Ihre App Snapchat kommt ausgesprochen schlicht daher. Ein kleiner Geist „Ghostface Chillah“, der als Maskottchen fungiert und nach dem Wu-Tang Clan Rapper „Ghostface

Killah“ benannt ist, bleibt die einzige jugendliche Extravaganz. Mit dem Programm kann man Fotos und Videos erstellen. Es bietet die Möglichkeit, den Account mit Twitter und Facebook zu vernetzen.

Das Besondere der Funktionsweise von Snapchat steht im krassen Gegensatz zur allgemeinen Praxis der Nutzung von Fotos im Internet: Eine Snapchat-Aufnahme ist grundsätzlich mit einem Haltbarkeitsdatum versehen. Das heißt: Der Nutzende bestimmt beim Erstellen der Nachricht, wie lange sein Foto oder Video den Empfangenden gezeigt werden soll – mindestens eine, maximal zehn Sekunden sind möglich. Danach zerstört sich die Nachricht von selbst. Völlig sicher ist der Dienst aber nicht. Die Betreiber versprechen, die übermittelten Bilder unmittelbar von ihren Servern zu löschen, doch ist es den Empfangenden eines Fotos durchaus möglich, einen Screenshot zu erstellen. Während die Mitteilung sich dann selbst zerstört, bleibt dieser auf dem Handy erhalten. Zwar erschwert die App das, indem sie den Nutzenden zwingt einen Button gedrückt zu halten, um die Fotos zu sehen, und warnt einen Nutzenden, wenn doch eine Kopie seiner Nachricht erstellt wurde, doch kann so ein Bild erhalten bleiben. Auch die Benachrichtigung beim Erstellen eines Screenshots können technisch Versierte umgehen.

Das Datensicherungsunternehmen Decipher Forensics meldete, es könne bei Smartphones, die mit Android laufen, Fotos im Nachhinein aus dem Speicher auslesen. Dazu benötige es nur ein entsprechendes Softwareprogramm und mindestens einen Tag Zugriff auf das Gerät; Snapchat benenne Fotos nur um, nachdem der Empfangende diese angesehen hat, so dass er sie nicht wiederfindet. Gelöscht würden sie nicht. Der Technologieblog Techcrunch hat versucht, den Test der Datensicherungsfirma zu wiederholen. Dabei ergab sich, dass die Experten ein übermitteltes, aber noch nicht geöffnetes Foto ansehen und umbenennen konnten – dies allerdings nur bei einem „gerooteten“ Smartphone, also einem Gerät, bei dem Voreinstellungen des Herstellers geändert und zusätzliche Rechte eingeräumt wurden. Ein gerootetes Handy lässt sich leichter von außen angreifen.

Snapchat trifft gerade bei jungen Menschen einen Nerv: Das Versenden erotischer Inhalte ist unter dem Begriff „Sexting“ bekannt geworden und unter Jugendlichen verbreitet. Snapchat ermöglicht das Versenden anstößiger Bilder verbunden mit der Erwartung, dass diese keine weitere Verbreitung finden. Das Team hinter Snapchat wehrt sich gegen die Vermutung, mit der App sollten vornehmlich anstößige Bilder verschickt werden. Der überwiegende Teil der Bilder werde tagsüber verschickt und ihr Inhalt sei lustig und nicht sexuell.

50 Millionen Fotos täglich wurden im Dezember 2012 via Snapchat ausgetauscht. Ein halbes Jahr später war von 150 Mio. und 200 Mio. pro Tag die Rede. Zum Vergleich: Instagrams Nutzer laden täglich gerade einmal fünf Millionen Fotos hoch. Zwar wirft Snapchat bislang keinen Profit ab, allerdings sammelten die jungen Entwickler bei einer ersten Finanzierungsrunde im Herbst 2011 immerhin rund eine halbe Million US-Dollar. Ende Juni 2013 waren es schon 60 Mio. US-Dollar. Facebook reagierte schnell und veröffentlichte mit dem Jahreswechsel 2012/2013 die eigene Foto-App Poke, die auch unabhängig vom sozialen Netzwerk funktioniert; seine Funktionen gleichen denen Snapchats bis ins Detail und auch Facebooks Gegenangriff ist kostenlos im App-Store verfügbar. Gerüchten zufolge hat Facebook seine App innerhalb kürzester Zeit auf den Markt geworfen – von nur drei Wochen Entwicklungszeit ist die Rede. Mark Zuckerberg selbst soll auf die rasche Fertigstellung gedrängt haben. Offenbar ist Facebooks CEO nicht bereit, alte Fehler zu wiederholen: Nach langem Zögern hatte Mark Zuckerberg für Instagram einen absurd hohen Preis bezahlt. Die Reaktion Zuckerbergs zeigt das enorme Potential, das Snapchat in der Branche zugesprochen wird (Wais, Smartphone-App Snapchat zerstört Fotos von selbst, www.welt.de

09.01.2013; Crocoll Digitale Selbstzerstörung, SZ 14.05.2013, 20; Huber, Der Vorzug der Vergänglichkeit, SZ 26.06.2013, 21).

## Angriff auf iOS durch manipulierte Smartphone-Steckdose

Forschende des Georgia Institute of Technology/USA haben angekündigt, öffentlich darzustellen, wie sich Geräte mit Apples Betriebssystem iOS durch ein manipuliertes Ladegerät mit schädlicher Software manipulieren lassen. Innerhalb nicht einmal einer Minute könne so jedes iPhone oder iPad zum offenen Buch für Hacker gemacht werden – allen Sicherheitsmaßnahmen wie etwa einer PIN-Sperre zum Trotz.

Dabei ist eine große Bandbreite vorstellbar, darunter Software, die Daten wie Kontakte, Mails und Ähnliches abgreift und über das Internet an die Angreifer versendet, ebenso wie Programme, die unbemerkt vom Nutzenden Mikrofon und Kamera der Geräte einschalten und es so als Wanze nutzen können. Die Wissenschaftler verwendeten für ihren Angriff eine nur wenige Zentimeter große Minicomputer-Platine, die es für 45 Dollar fertig zu kaufen gibt.

Die Forschenden beschreiben, dass sie diese Hardware ausgesucht haben, um zu zeigen, wie leicht es ist, ein unverdächtig aussehendes USB-Ladegerät zu bauen, in dem die Platine zusammen mit Bauteilen für ein echtes Ladegerät in einem Gehäuse verbaut wird. Steckt man ein Apple-Gerät an diese Konstruktion, lässt sich beliebige Software auf jedes Gerät laden, das mit iOS läuft. Die Forschenden konnten die eingeschleuste Software tief im System verankern, so dass sie nur sehr schwer zu finden war. Der Angriff funktioniert deshalb, weil die Buchse, an die man das Ladegerät anschließt, nicht bloß für die Stromversorgung zuständig ist. Darüber lassen sich die Geräte auch mit Computern verbinden, zum Beispiel um Musik zu überspielen. Bis Ende Juli 2013, wenn die Forschenden ihre Erkenntnisse im Detail öffentlich machen, hat Apple nun Zeit, sich Gegenmaßnahmen auszudenken.

Die Sicherheitsforscher Sebastian Schreiber und Philipp Buchegger berichten über eine ähnliche Sicherheitslücke: Ihnen ist es gelungen, ein komplettes Backup der Daten von IPhones und iPads zu ziehen, selbst wenn das Gerät

gesperrt war. Auch das spätere Ändern des Sperrcodes nützt den Besitzenden nichts, weil das Netzteil sich den Masterschlüssel ergattert. Deshalb gibt Schreiber den Ratschlag: „iPhones und iPads sollten ausschließlich mit eigenen vertrauenswürdigen Geräten verbunden werden“ (Martin-Jung, Handy-Attacke aus der Steckdose, SZ 05.06.2013, 10; Datenklau von iPhones und iPads, Der Spiegel 24/2013, 106).

## Pulsmessen per Webcam

2012 haben Informatiker um Michael Rubinstein vom Massachusetts Institute of Technology (MIT) eine Methode der Eulerschen Videoverstärkung (EVM) vorgestellt, die kleinste Bewegungen verdeutlicht. Mit der Methode des Computer Science and Artificial Intelligence Laboratory (CSAIL) lassen sich aus Videodaten Veränderungen herausfiltern und verstärken. Verborgene Vorgänge in Gebäuden und Gerüsten sind dadurch zu erkennen. In Gesichtern ist mit etwas Verstärkung auch der Pulsschlag erkennbar. Im März 2013 veröffentlichten die Forschenden den Quellcode ihrer Arbeit, was nun andere Programmierer animierte, die Technik weiterzuentwickeln und zu Forschungszwecken auf haushaltsüblichen Geräten nutzbar zu machen.

Der NASA-Forscher und Programmierer Tristan Hearn (thearn) veröffentlichte ein von der EVM inspiriertes Programm für Webcams, das automatisch das Gesicht des Nutzenden erkennt, sich eine Stelle auf der Stirn sucht und anhand der Farbveränderungen durch einströmendes Blut den Pulsschlag zu berechnen beginnt. Im Test schwanken die Werte zwar, sobald der Kopf bewegt wird. Bei einem sich nicht bewegenden Probanden berechnet das Programm aber erstaunlich gut den Herzschlag: Die Pulsfrequenz nach einem Sprint durchs Treppenhaus gab die Software bis auf einige Schläge pro Minute genau an. Hearn bietet seinen Webcam-Puls-Detektor kostenlos zum Herunterladen an.

Dadurch wirft er eine Frage auf, die in der aktuellen Debatte um Gesichtserkennung, etwa über die derzeit getestete Google-Brille, wichtig werden könnte: Sind abseits der Personenerkennung die Gesichtsdaten auch für andere Zwecke tabu? Schickt es sich beispielsweise, beim Flirten per Webcam den Erregungsgrad des Gegenübers zu messen? Ende Mai 2013 verbot Google zwar in seinen Richtlinien Apps, die Benutzer namentlich identifizieren, aber über weitere Analysen von Gesichtsdaten macht das Unternehmen keine konkreten Aussagen. Beim Ideenwettbewerb zur Einführung der Brille fand der Anwendungsbereich der Telemedizin, also die Diagnose über Videozuschaltung, großen Anklang und Beachtung.

Elektrotechniker Christian Hofmann vom Fraunhofer Institut für Integrierte Schaltungen sieht darin ein „großes Zugpferd für medizinische Sensorik“. Mit Kollegen in Erlangen erforscht er neue Geräte und Plattformen, aber auch Methoden zur medizinischen Datenverarbeitung. In einer immer älter werdenden Gesellschaft werde der Bedarf an schnellen und flächendeckenden Videodiagnosesystemen zukünftig immer größer: „Der von den Amerikanern offengelegte Quellcode ist da sicherlich ein Multiplikator. Studenten und Forscher können so schnell und unkompliziert damit arbeiten und entwikkeln.“ Aussagekräftig und medizinisch nützlich sind solche Programme insbesondere, wenn viele Daten zusammenfließen und kombiniert analysiert werden, so Hofmann: „Wenn ich den Puls einer Person messe, kenne ich nur einen Wert. Messe ich auch die Bewegung, kann ich folgern: Der Puls ist erhöht, weil die Person rennt.“ Daraus könne sich ein Missbrauchspotential ergeben. Zusammen mit anderen Daten könnte die Software eine Basis liefern für Stressanalysen und Lügendetektoren, die das Gegenüber bewerten – und das womöglich ganz unauffällig, zum Beispiel mit einem kleinen Programm auf der Datenbrille (Gotzner, Open-Source-Software: Webcam fühlt den Puls des Nutzers, www.spiegel.de 06.06.2013).

## Digitale Video-Stressdetektion für Studierende

US-Forschende wollen Lernsysteme mittels Bilderkennung so verbessern, dass sie künftig automatisch reagieren, wenn eine SchülerIn nicht mitkommt. Die in der North Carolina State University (NCSU) entwickelte Hard- und Softwarekombination soll Lehrkräften helfen, gestresste Lernende besser zu erkennen – beispielsweise bei E-Learning-Anwendungen, wo die Lernenden sich nicht mehr im Klassenraum befinden. Das Verfahren nutzt Kameras, die die Gesichter der Lernenden während eines Seminars erfassen. Mit einer Software, die darauf trainiert ist, Gesichtsausdrücke mit verschiedenen Abstufungen des menschlichen Stressniveaus zu korrelieren, wird das Bildsignal dann später analysiert. So lässt sich erkennen, welche Studierenden Probleme hatten und welche die Arbeit eher für zu einfach hielten.

Das NCSU-Team gab Studierenden die Aufgabe, mit der Lernsoftware „JavaTutor“ zu trainieren, Code in der Programmiersprache Java zu schreiben. Anschließend wurden insgesamt 60 Stunden dabei aufgezeichnetes Videomaterial mit der Computer Expression Recognition Toolbox überprüft, die Gesichtsausdrücke einordnen kann. Die Rückschlüsse, die die Software zog, wurden dann mit von den Studierenden selbst erfassten Gefühlszuständen abgeglichen. Beides war nahezu deckungsgleich. Gemäß Joseph Grafsgaard, Doktorand an der NCSU und Co-Autor der Studie, ist es das Ziel, ein Tutorsystem zu entwickeln, das Studierenden direkt hilft, die Schwierigkeiten haben, und ihnen wieder „Selbstvertrauen und Motivation“ zu geben. Verschiedene andere Wissenschaftlergruppen untersuchen ebenfalls, ob sich dieses sogenannte Affective Computing im Bildungsbereich nutzen lässt. Jacob Whitehill, Softwareingenieur und Forscher beim Start-up Emotient, hat kürzlich an einer Untersuchung teilgenommen, die zeigen sollte, ob die Analyse des Gesichtsausdruckes eines Menschen durch Software sinnvolle Rückschlüsse auf Prüfungsergebnisse zulässt (Kamerasystem ermittelt Lernstress, www.heise.de 15.07.2013; Knight, Gesichtserfassung erkennt überforderte Studenten, www.heise.de 15.07.2013).

## Spracherkennung per Videokontrolle

Auf einem internationalen Akustikkongress in Kanada präsentierte der Ingenieur Yasuhiro Oikawa von der japanischen Waseda-Universität, dass durch Analyse der Vibrationen am Hals einer Redenden erkannt werden kann, was diese sagt. Oikawas Hochgeschwindigkeitskamera erstellt 10.0000 Bilder pro Sekunde, während eine Testperson spricht. Am Rechner können dann diese Kamerabilder in Sprache übersetzt werden. Bisher ist es Oikawa gelungen, mit dieser Methode lediglich einzelne Worte zu rekonstruieren; ganze Sätze sollen folgen (Der Spiegel 25/2013, 95).

## Personenortung durch Wände per W-LAN

Anfang Juni 2013 stellten Forschende der University of Washington/USA eine durch Wände funktionierende Gestensteuerung per W-LAN vor. Kurz danach zeigten Informatiker des Massachusetts Institute of Technology/USA, wie sich W-LAN-Strahlung zur Ortung von Personen hinter verschlossenen Türen nutzen lässt. Die Informatiker Dina Katabi und Fadel Adib stellten ihr „Wi-Vi"-Projekt vor, das Personen hinter Wänden orten kann. Die Forschenden des Computer Science and Artificial Intelligence Laboratory (CSAIL) entwickelten dafür eine Software, die Reflektionen und Veränderung der elektromagnetischen Strahlung, die von einem kabellosen Router ausgeht, nutzt.

Ein sich bewegender menschlicher Körper beeinflusst die Funksignale. So lassen sich Ort und Bewegung einer Person anhand der Signalmuster bestimmen. Auch die Anzahl der Personen im Raum wollen die Forschenden mit Hilfe der Strahlung auswerten können. In einem YouTube-Video demonstrieren sie, wie ein durch einen Raum gehender Mann das Signalbild verändert. Wi-Vi ist demgemäß nur auf einen Empfänger angewiesen, um eine Person zu verfolgen. Die vom Körper reflektierte Strahlung und ihre sich verändernde Laufzeit zur Empfangsstation seien ausreichend, um Position und Bewegung zu bestimmen. Als Anwendungsbereich ihrer Technik sehen die Forschenden unter anderem Rettungs- und Bergungsoperationen. Die Ortung verschütteter Personen könnte so auch durch Objekte oder Hindernisse hindurch funktionieren. In der Sicherheitstechnik wären Wi-Vi-Systeme als flächendeckende Bewegungssensoren für Gebäude denkbar. Katabi und Adib präsentieren ihre Technik auf der SIGCOMM 2013, einer Konferenz für Datenkommunikation im August 2013 in Hongkong (Ortung von Personen: Mit W-Lan durch Wände sehen, www.spiegel.de 05.07.2013).

# Rechtsprechung

### EGMR

## Keine Internetlöschung wegen schlechter Presserecherche

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg stellte in einer Kammerentscheidung vom 16.07.2013 fest, dass Zeitungen in Europa nicht verpflichtet sind, Artikel aus dem Internet zu nehmen, wenn ein Gericht sie als rufschädigend eingestuft hat (Wegrzynowski et Smolczewski c. Pologne, 33846/07). Der Fall drehte sich um die polnische Tageszeitung Rzeczpospolita und ihre Berichterstattung über zwei Anwälte und angeblich fragwürdige Geldgeschäfte. Polnische Gerichte stellten 2002 fest, dass der Text nicht gründlich recherchiert worden sei und Persönlichkeitsrechte verletze. Im Netz blieb er trotzdem weiter zu lesen. Die Kammer des EGMR meinte, dass hier die Informationsfreiheit gegenüber dem Schutz des Rufs und der Privatsphäre überwiege. Ebenso wie das Regionalgericht von Warschau vertrat sie die Ansicht, dass es nicht die Aufgabe der Justiz sei, durch Löschen von erfolgten Meldungen die Geschichte neu zu schreiben. Die Öffentlichkeit habe ein legitimes Interesse am Zugang zu elektronischen Pressearchiven, was durch die Meinungsfreiheit des Art. 10 der Europäischen Menschenrechtskonvention geschützt ist. Es sei jedoch wünschenswert, dem Persönlichkeitsrechte verletzenden Artikel einen Kommentar hinzuzufügen, in dem darüber informiert wird, dass in einem Zivilverfahren den Klägern bezüglich der Geltendmachung ihrer Persönlichkeitsrechte wegen des Artikels Recht zugesprochen worden ist (EuGH: Artikel müssen nicht gelöscht werden, SZ 17.07.2013, 31).

### EuGH

## Millionenstrafe gegen Schweden wegen verspäteter Vorratsdatenspeicherung

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 30.05.2013 entschieden, dass Schweden eine EU-Strafe von 3 Millionen Euro zahlen muss, weil das Land die EU-Richtlinie von 2006 zur Vorratsdatenspeicherung nur mit Verspätung umgesetzt und somit europäisches Recht verletzt habe

(Az. C-270/11). Die EU-Richtlinie von 2006 (2006/24/EG) schreibt den Staaten vor, Verbindungsdaten ihrer BürgerInnen (Funkzellen, Standortkennung, IP-Adressen usw., nicht Kommunikationsinhalte) zu Fahndungszwecken anlasslos für mindestens sechs Monate zu speichern. Viele sehen darin einen übermäßigen Angriff auf das Grundrecht auf Datenschutz. Nach Ansicht des EuGH wirken sich Verzögerungen bei der Umsetzung des EU-Gesetzes negativ auf die Arbeit von Justiz und Polizei aus, die schwere Straftaten nicht so leicht aufdecken könnten. Schweden habe „erhebliche Zeit", nämlich fast fünf Jahre, abgewartet, bis das Land begonnen habe, Vorratsdaten zu speichern.

Der Fall ist für Deutschland von Bedeutung, da auch dieses Land im Mai 2012 von der EU-Kommission verklagt worden ist. Weil nach der Aufhebung der nationalen Regelung durch das Bundesverfassungsgericht keine Neuregelung erfolgt ist, wird auch hier nach Ansicht der EU-Kommission EU-Recht verletzt, so dass ebenfalls ein millionenschweres Bußgeld droht, das aber erst nach einem Urteil fällig würde. Eine Neuauflage scheiterte bisher daran, dass sich die CDU/CSU-Fraktion bei der Durchsetzung der Richtlinie gegenüber der FDP nicht durchsetzen konnte. Die umstrittene EU-Richtlinie sollte eigentlich bereits 2012 überarbeitet werden. EU-Kommissarin Cecilia Malmström hatte angekündigt, die Speicherdauer einschränken zu wollen. Bisher sind zwischen sechs Monate und zwei Jahre vorgeschrieben. Außerdem könnte es Auflagen geben, wie die Daten sicher gespeichert werden müssen (Schweden: EU-Millionenstrafe für späte Vorratsdatenspeicherung, www.spiegel.de, 30.05.2013)

### BGH

## Google muss bei Autocomplete Persönlichkeitsrechte beachten

Der Bundesgerichtshof (BGH) entschied mit Urteil vom 14.05.2013, dass Google automatische Suchvorschläge (Autocomplete) entfernen muss, wenn sie Persönlichkeitsrechte verletzen (Az. VI ZR 269/12). Sobald der Suchmaschinenbetreiber über solch eine Rechtsverletzung informiert ist, ist er verpflichtet, sie für die Zukunft zu verhindern. Der BGH gab einem Unternehmer als Kläger Recht, der sich durch die automatische Ergänzung seines Namens um zwei Suchbegriffe in seinen Persönlichkeitsrechten verletzt sah. In den ersten beiden Instanzen vor dem Landgericht und dem Oberlandesgericht (OLG) Köln war er noch unterlegen. Der BGH verwies den Fall an das Berufungsgericht zurück.

In dem konkreten Fall fühlte sich der Kläger durch die automatische Vervollständigung seines Namens um die Begriffe „Scientology" und „Betrug" in seinen Rechten verletzt. Er behauptet, weder in irgendeinem Zusammenhang mit Scientology zu stehen, noch sei ihm ein Betrug vorzuwerfen. Es stelle auch keines der Suchergebnisse einen solchen her. Google hatte dagegen argumentiert, dass die Suchvorschläge ohne Wertung die gegenwärtigen Suchvorlieben im Netz widerspiegeln. Dieser Auffassung hatte sich das OLG angeschlossen. Der BGH stellte fest, dass die Kombination des Namens mit den negativ besetzten Begriffen einen „fassbaren Inhalt" hat, der das Persönlichkeitsrecht des Betroffenen verletzen kann.

Die Frau des ehemaligen Bundespräsidenten, Bettina Wulff, hatte im September 2012 ebenfalls Google verklagt, weil die Suchmaschine bei Eingabe ihres Namens diesen automatisch um Begriffe wie „Escort" ersetzt. Ihr Verfahren wurde im April 2013 verschoben, um die Entscheidung des BGH abzuwarten.

Der BGH betonte allerdings, dass Google nicht für jede Persönlichkeitsrechtsbeeinträchtigung durch Suchvorschläge haftet: „Der Beklagten (Google) ist nämlich nicht vorzuwerfen, dass sie eine Suchvorschläge erarbeitende Software entwickelt und verwendet hat, sondern lediglich, dass sie keine hinreichenden Vorkehrungen getroffen hat, um zu verhindern, dass die von der Software generierten Suchvorschläge Rechte Dritter verletzen." Nehme ein Betroffener den Betreiber einer Internet-Suchmaschine mit Suchwortergänzungsfunktion auf Unterlassung der Ergänzung persönlichkeitsrechtsverletzender Begriffe bei Eingabe des Namens des Betroffenen in Anspruch, setze die Haftung des Betreibers die Verletzung zumutbarer Prüfpflichten voraus: „Der Betreiber einer Suchmaschine ist regelmäßig nicht verpflichtet, die durch eine Software generierten Suchergänzungsvorschläge generell vorab auf etwaige Rechtsverletzungen zu überprüfen. Der Betreiber ist grundsätzlich erst verantwortlich, wenn er Kenntnis von der rechtswidrigen Verletzung des Persönlichkeitsrechts erlangt."

In einer ersten Stellungnahme zeigte sich Google-Sprecher Kay Oberbeck enttäuscht von der BGH-Entscheidung. Erfreulich sei zwar, „dass das Gericht die Autovervollständigung für zulässig hält und Google nicht verpflichtet, jeden angezeigten Begriff vorab zu prüfen." Nicht nachvollziehen könne Google aber die Auffassung des BGH, „dass Google für die von Nutzern eingegebenen Suchbegriffe dennoch haften soll. Denn bei den Autovervollständigungen handelt es sich um automatisch angezeigte Begriffe, die Google-Nutzer zuvor gesucht haben." Er wies darauf hin, dass Google schon jetzt auf Hinweise zu Urheberrechtsverletzungen reagiere und solche Seiten als Suchergebnisse tilgt, die illegale Downloads ermöglichen. Nutzende, die sich durch die Google-Funktion in ihren Persönlichkeitsrechten verletzt fühlen, müssen sich jetzt über ein schwer auffindbares Formular beim Konzern direkt beschweren. Das Gesuch wird dann von der zuständigen Rechtsabteilung geprüft. Gegebenenfalls würde auch Hilfe externer Kanzleien eingeholt. Inwieweit Google nun technisch oder organisatorisch auf die Entscheidung weiter reagiert, ließ Oberbeck offen. Bundesjustizministerin Sabine Leutheusser-Schnarrenberger lobte die Stärkung der Persönlichkeitsrechte durch den BGH: „Gut, dass Google jetzt arbeiten muss" (Janisch, Niederlage für Google, SZ 15.05.2013, 1, 4, PE BGH, Bundesgerichtshof entscheidet über die Zulässigkeit persönlichkeitsrechtsverletzender Suchergänzungsvorschläge bei „Google" 15.05.2013;

BGH zu Autocomplete: Google muss in Suchvorschläge eingreifen, www.heise.de 16.05.2013; Google ist, Der Spiegel 21/2013, 133).

BGH

## Peilsendereinsatz durch Detektive grundsätzlich strafbar

Der Bundesgerichtshof (BGH) stellte mit Urteil vom 04.06.2013 klar, dass die Überwachung von Personen mit Peilsendern grundsätzlich nach den §§ 44 i. V. m. 43 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) strafbar ist und nur in absoluten Ausnahmefällen gerechtfertigt sein kann (1 StR 32/13). Lediglich bei einem „starken berechtigten Interesse" – also notwehrähnlichen Situationen, in denen zum Beispiel die berufliche Existenz auf dem Spiel steht – könne dies erlaubt sein. Dazu zähle aber auf gar keinen Fall eine Observation etwa von Eheleuten, die sich der Untreue verdächtigen. Der BGH bestätigte damit im Grundsatz ein Urteil des Landgerichts (LG) Mannheim aus dem Jahr 2012, in dem zwei Detektive zu Bewährungsstrafen verurteilt worden waren. Ein Teil der seinerzeit verhandelten Fälle wurden jedoch an das LG zurückverwiesen. Dort muss die Frage eines „berechtigten Interesses" geklärt werden, was bisher nicht ausreichend erfolgte. Soweit nach den Urteilsfeststellungen die Annahme eines berechtigten Interesses von vornherein ausgeschlossen war, hatten die Schuld- und Einzelstrafaussprüche des LG Bestand.

Die beiden Privatermittler einer Stuttgarter Detektei hatten an den Autos ihrer „Zielpersonen" GPS-Sender (Global Positioning System) angebracht und damit Bewegungsprofile erstellt. Unter anderem sollte die Untreue von Eheleuten nachgewiesen werden. Außerdem wurden krankgeschriebene Beschäftigte überwacht; zudem sollten im Auftrag eines Labors über Mitarbeitende einer Krankenkasse kompromittierende Daten gesammelt werden. Einer der beiden Detektive meinte vor Gericht: „Wenn ich gewusst hätte, dass ich GPS nicht verwenden darf, hätte ich das nicht gemacht." Die Überwachung per Peilsender ist gemäß dem BGH-Urteil ein schwerwiegender Eingriff in das Persönlichkeitsrecht des Betroffenen: „Wenn man nicht weiß, ob so was erlaubt ist, dann muss man es lassen." Die Anwältinnen der Detektive hatten zuvor die bisherige unklare Rechtsprechung moniert und argumentiert, dass GPS-Daten keine personenbezogenen Daten und zudem allgemein zugänglich seien. Auch dem widersprach der BGH: Der Personenbezug sei mit dem Einsatz des GPS von vorneherein gegeben. Auch seien diese Daten schon deshalb nicht für jedermann zugänglich, weil sie nur mithilfe des heimlich in ein fremdes Auto eingebauten Senders gewonnen werden könnten.

Andreas Heim vom Bund Internationaler Detektive (BID) kommentierte die strafbare Praxis: „Wir machen höchstens Bilder und sprechen unsere Erkenntnisse auf ein Diktiergerät. Der Einsatz von GPS-Systemen ist tabu." Generell müssten sich Detektive auf das Hören, Sehen und Beobachten verlassen. Auch Horst Probst vom Bundesverband Deutscher Detektive (BDD) betonte: „Im Zweifel Finger weg von technischen Hilfsmitteln" (BGH verbietet Peilsender, www.n-tv.de, 04.06.2013; Überwachung von Personen mittels an Fahrzeugen angebrachter GPS-Empfänger ist grundsätzlich strafbar, www.kostenlose-urteile.de, 04.06.2013; Peilsender verboten, SZ 05.06.2013, 6).

BGH

## Kein Ersatz für Detektiv-GPS-Überwachungskosten

Ein geschiedener Ehemann darf gemäß einem Beschluss des Bundesgerichtshofes (BGH) vom 15.05.2013 im Unterhaltsstreit mit seiner Ex-Frau einen Detektiv einsetzen und ihr die Kosten dafür in Rechnung stellen. Dies gilt jedenfalls dann, wenn er durch den Detektiveinsatz nachweisen kann, dass die ehemalige Gattin mit einem anderen Mann zusammenlebt. Detektivische Beobachtungen sind demnach erlaubt und erstattungsfähig – der Einsatz von GPS-Sendern für ein umfassendes Bewegungsprofil jedoch nicht (Az. XII ZB 107/08).

Der Kläger war zur Zahlung von nachehelichem Unterhalt verurteilt worden. Seine Ex-Frau hatte in dem Verfahren angegeben, ihre Beziehung zu einem anderen Mann sei inzwischen beendet. Später lebte die Frau aber wieder mit dem neuen Partner zusammen. Damit war auch der Anspruch auf Geld vom Ex-Mann verwirkt. Zur Vorbereitung einer Abänderungsklage engagierte dieser ein Detektivbüro und wollte die Überwachungskosten später von der Frau erstattet haben. Gemäß dem Urteil des BGH ist dies grundsätzlich möglich. Zu den Prozesskosten könnten auch Kosten gehören, „die durch rechtmäßige Maßnahmen zur Vorbereitung eines bevorstehenden Verfahrens ausgelöst werden". Dazu könnten auch Detektivkosten gehören, wenn sie auf der Grundlage eines konkreten Verdachts zur Durchsetzung des Rechts notwendig gewesen seien. Bedingung sei allerdings, dass sich die Detektivkosten „in angemessenem Verhältnis zur Bedeutung des Streitgegenstandes halten und die erstrebte Feststellung nicht einfacher oder billiger zu erzielen war."

Die Frau muss im entschiedenen Fall nicht die komplette Rechnung des Detektivbüros begleichen. Die ausgespähten Partner müssten nur die Kosten für die vor Gericht zulässigen Beweismittel tragen. Mit GPS-Sendern erstellte Bewegungsprofile zählten nicht dazu, weil sie gegen das Recht auf informationelle Selbstbestimmung der Betroffenen verstoßen. Zulässig sei dagegen eine „punktuelle persönliche Beobachtung" der Ex-PartnerIn. Auch damit könne bewiesen werden, dass der oder die Ex wieder in einer „verfestigten" Gemeinschaft lebt. Am 04.06.2013 urteilte der BGH, dass Privatdetektive generell keine Peilsender einsetzen dürfen, um Personen zu überwachen. Lediglich bei einem „starken berechtigten Interesse" – also notwehrähnlichen Situationen, in denen zum Beispiel die berufliche Existenz auf dem Spiel stehe – könne dies erlaubt sein (s.o. Az. 1 StR 32/13; BGH-PE Nr. 121/13 12.07.2013, Detektivkosten im Unterhaltsrechtsstreit juris.bundesgerichtshof.de; Muss Ex-Frau ihre Überwachung bezahlen? www.n-tv.de 12.07.2013).

# Buchbesprechung




Kutscha, Martin/Thomé, Sarah
**Grundrechtsschutz im Internet?**
Nomos Verlag Baden-Baden, 2013,
ISBN 978-3-8329-7907-2, 153 S.

tw – Es kommt nicht von ungefähr, dass die beiden AutorInnen ihren Titel „Grundrechtsschutz im Internet?" mit einem Fragezeichen versehen haben. Zwar gibt es manchen Anlass für einzelne Ausrufezeichen, und das Buch ist hierfür ein Beleg, doch belegt es zugleich die bestehenden Defizite. Es ist in zwei Teile geteilt. Im ersten dekliniert Martin Kutscha unsere für das Internet wesentlichen Grundrechte mit juristischer Routine durch. Im zweiten Teil befasst sich Sarah Thomé weniger umfassend mit praktischen und institutionellen Problemen des Datenschutzes im Internet.

Eigentlich sollte es selbstverständlich sein, dass das Internet kein (grund-) rechtsfreier Raum ist, zumal wenn das Internet in Deutschland, einem ausgewiesenen Rechtsstaat, zum Einsatz kommt. Doch Ubiquität, Intransparenz, technische Konvergenz und Globalität sind teilweise ungeklärte Herausforderungen für die Durchsetzung des Rechts und der Grundrechte. So ist von hoher praktischer Relevanz, dass rechtlich nicht oder nur schwer zu greifende aus den USA heraus agierende globale Unternehmen die Internetdatenverarbeitung dominieren und bestimmen. Kutscha nähert sich dieser wie einer Vielzahl weiterer praktischer Phänomene, etwa den erweiterten staatlichen Ermittlungsmöglichkeiten per Online-Durchsuchung oder E-Mail-Beschlagnahmen oder den auftauchenden Interessensabwägungsproblemen, in einer unaufgeregten und zugleich sehr engagierten rechtlichen Weise. Er unterscheidet sich dadurch wohltuend von vielen ideologisch und kommerziell motivierten Menschheitsbeglückern und Besserwissern, die immer noch die öffentliche Debatte bestimmen.

Kutscha leitet das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme historisch und dogmatisch ab und stellt diese Persönlichkeitsrechte sowie das Telekommunikationsgeheimnis ins Verhältnis zu anderen Grundrechten, etwa die Informations- und Meinungsfreiheit oder die wirtschaftlichen Rechte auf Schutz des Urheberrechts, des Eigentums und des Berufs. Er stellt die berechtigte Frage, inwieweit die Grundrechte dem Staat im Hinblick auf die Nutzung des Internets grundrechtlich begründete Gewährleistungspflichten auferlegt. Zugleich kritisiert er die lauter werdenden Stimmen der Relativierung der Menschenwürdegarantie und – m. E. nicht zu Recht – die durch das BVerfG aufgrund der informationstechnischen Gegebenheiten zwangsläufig vorgenommene Aufweichung des Kernbereichsschutzes.

Sarah Thomé befasst sich mit den institutionellen Defiziten beim Grundrecht auf Datenschutz, die für sie vorrangig folgende sind: Ungenügende Unabhängigkeit, Trennung zwischen öffentlichem und privatem Bereich und unzureichende Sanktionsmöglichkeiten. Sie thematisiert die nationalen Grenzen der Aufsicht angesichts internationalen Datenverkehrs und sucht rechtliche Anknüpfungspunkte für die Kontroll- und Sanktionstätigkeit. Realistisch werden bestehende Datenschutzinstrumente wie z. B. Safe Harbor oder die Angemessenheitsprüfung ausländischer Datenschutzstandards problematisiert, ohne aber eigene klare Kanten zu ziehen, wie hier rechtspolitisch und rechtspraktisch vorgegangen werden kann und sollte. So ist die LeserIn zwar nach der Lektüre besser informiert, aber nicht gerade ermutigt.

Tatsächlich ist das Buch nicht als Kampfschrift konzipiert und geeignet, wenngleich viele, vor allem die rechtlichen Argumente für den Kampf für digitale Grundrechte, zum Ansatz gebracht werden können. Es will auch keine umfassende Abhandlung zum Grundrechtsschutz im Internet sein. Wohl aber bereitet es viele gute Informationen und Argumente für die Erörterung dieses Themas auf und ist insofern zu empfehlen. Es gibt noch einiges zu tun, bis beim Titel das Fragezeichen durch viele Ausrufezeichen ersetzt ist.




Heuer, Steffan/Tranberg, Pernille
**Mich kriegt Ihr nicht! Gebrauchsanweisung zur digitalen Selbstverteidigung**,
Murmann, Hamburg 2013,
ISBN 978-3-86774-243-6, 238 S.

tw – Das Buch ist einerseits mehr – andererseits weniger als der Untertitel verspricht: Es ist mehr, weil es quellen- und umfangreich in einer leicht verständlichen klaren Sprache darüber informiert, wie im Internet gegen den Datenschutz

nach modernem europäischen Verständnis verstoßen wird. Es ist weniger, weil es nur auf 30 Seiten – das aber äußerst kenntnisreich und nachvollziehbar – darstellt, mit welchen technischen Selbstschutzmaßnahmen die Privatsphäre im World Wide Web verteidigt werden kann. Bevor es also Therapievorschläge macht, erfolgt eine ausführliche Diagnose. Diese ist auf dem Stand der aktuellen Medien-Berichterstattung über Internetdatenschutz – vor Snowden. Mir ist keine derart konsistente Darstellung der aktuellen Trends und Fakten in Bezug auf die legale und illegale informationelle Fremdbestimmung und Ausbeutung bekannt. Wer insofern täglich die Online-Medien verfolgt, findet hier viel wieder und erfährt allenfalls wenige neue Details. Adressaten des Buches sind aber nicht primär die Nerds, sondern die durchschnittlichen Internet-UserInnen. Und diese werden hier bestens informiert – zum Identitätsklau, zur Kommerzialisierung digitaler Daten, zur Datennutzung durch Arbeitgeber, zu den Datenschutzproblemzonen von Smartphones und Handys, zum Tracking und Profiling, zur Nutzung des Internet für Zwecke der Unterhaltung, der digitalen Körperüberwachung, der sozialen und Beziehungskommunikation. Die Themen Mobbing, Anonymität im Netz und digitaler Tod werden behandelt.

Im kürzeren zweiten Teil nennen die beiden AutorInnen, ein deutscher Journalist in den USA und eine dänische Kollegin, in vier Qualitätsstufen Tipps und Trick, indem sie Werkzeuge zum Schutz informationeller Selbstbestimmung im Netz präsentieren. Auch hier ist wieder nicht der Freak Adressat, sondern die Normal-UserIn, wobei die AutorInnen mit ihren Schritt-auf-Schritt-Hinweisen, der Nennung von hilfreichen Webseiten und Tools der Nutzenden von Facebook, Google & Co. sowie der Erklärung von deren Funktionieren und deren Hintergründe nicht nur brauchbare Anleitungen geben, sondern zugleich zum Verständnis der Selbstschutzmechanismen beitragen. Das Werk ist als Hilfe zur Selbsthilfe angelegt, macht keine politischen, moralischen oder detaillierte rechtlichen Ausführungen. Es ist aber eine klare Parteinahme für den Datenschutz und gegen die kommerzielle und staatliche Ausbeutung der UserInnen-Daten. Insofern kommt es – nach Bekanntwerden des Prism/Tempora-Komplexes – genau zur richtigen Zeit und füllt eine Marktlücke, indem es Fragen beantwortet, die sich UserInnen mit Bekanntwerden der Snowden-Enthüllungen erstmals stellen, wenngleich das Buch vor Bekanntwerden der Details von der flächendeckenden Internetüberwachung verfasst wurde. Nur manchmal scheint es insofern etwas eindimensional, dass es allzu überzeugt zu sein scheint, dass der Datenschutz im Internet sich immer stärker durchsetzen wird. Doch dieser Zweckoptimismus wird nicht übertrieben; das Buch selbst ist ein Beleg für diese These. Die ideale Geschenkidee für erwachsene kritische Internet-UserInnen, die es – statt nur immer die Oberfläche von Bildschirmen und Displays zu sehen – erstmals genauer wissen wollen.

## Cartoon








Foto: David Valenta